DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

1. TITLE	2. IDENTIFICATION NUMBER
FORMAL SECURITY POLICY MODEL	DI-MISC-81346

3. DESCRIPTION/PURPOSE

3.1 A Formal Security Policy Model is a mathematically precise abstract representation of a security policy and the abstract protection mechanisms that enforce the policy. To be acceptable as a basis for a trusted computing base (TCB), the model must be supported by formal proof. This Data Item Description (DID) describes both the requirements for the model itself and the document in which the model will be delivered.

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 3.1.4.4, 3.1.3.2.2, 3.2, 3.2.3.2.2, 3.2.4.4, 3.3.3.2.2 and 3.3.4.4 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 formal security policy model as specified by DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) for TCB Classes B1 (Labeled Security Protection), B2

(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6936

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 Formal Computer Security Policy Model 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, and any other appropriate descriptive data.

b. Errata Sheet. Errata sheets shall contain 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 security model, including its assumptions and limitations.

(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)

(Structured Protection), B3 (Security Domains), or A1 (Verified Design) products or their equivalent systems. The Formal Security Policy Model is an optional requirement at TCSEC Class B1. If an Informal Security Policy Model is required and available at TCSEC CLASS B1, then the Formal Security Policy Model is redundant and not necessary. The Formal Security Policy Model is based on the Philosophy of Protection Report.

Block 10, PREPARATION INSTRUCTIONS (Continued)

g. Introduction.
h. Body of the Report.
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. Black 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.

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 12 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 each page to allow for drilling and binding.

i. The report shall be provided in standard three-ring notebook binders for ease of maintenance.

j. The report shall be provided in standard three-ring notebook binders for ease of maintenance.

10.3 General. The formal Security Policy Model document shall contains the formal security policy model, it s associated proofs, and the supporting explanations and documentation for both the model and proofs. The model contained in the Formal Security Policy Model document consists of two segments: 1) the mathematical representation of the policy which is to be enforced by the TCB, and 2) a mathematical representation of the abstract protection mechanism(s) within the TCB which enforce the described policy. The model shall include the representation of subjects, objects, modes of access, and security labels; the set of security properties enforced by the TCB; the representation of the initial state of TCB; and the representations of the operations performed.

Block 10. PREPARATION INSTRUCTIONS (Continued)

10.4 Content. The Formal Security Policy Model document shall provide background information supporting the modeling effort. All of this background information is informal in nature and may be presented in English text, and graphic representations where appropriate. The following items shall be included as part of this information:

a. Summarization of the security policy to be modeled, how this policy relates to the overall security policy (if the policy modeled is some subset of the overall policy), and the source of the policy. This discussion shall be in enough detail to form the background for the model.

b. Discussion in detail of the type of model chosen, and explanation of why this type was selected over other types.

c. Identification of the modeling technique/methodology chosen, and why it was chosen.

d. Expansion of the security policy into security policy statements. These security policy statements may be brief, but they must explicitly and thoroughly describe the security policy. Each policy statement shall be mapped to the Philosophy of Protection Report.

10.4.1 Policy segment. The Formal Security Policy Model document shall provide a formal mathematical description of the policy enforced by the TCB. Also, an English language description of the formal security policy model and each of its segments shall be provided. Supporting material should be provided in the following sequence:

a. All assumptions used in the model, provided as both mathematical statements (if any) and an English language description. Sufficient supporting rationale to prove the validity of the assumptions shall be provided. An explanation of why the assumptions are necessary to the model and the consequences of violating the assumptions shall also be provided.

b.All axioms used in the model, using both mathematical statements and an English language description. This discussion shall include the rationale as to why these axioms are needed and how the axioms are justified. Supporting rationale for each axiom shall be provided by describing its relationship to the model's segments and specific security-enforcement abstract mechanisms in the model.

c. The actual model of the policy. Graphic representations of the model's segments may be included (e.g., diagrams and tables). These graphics shall be annotated with English language descriptions. Supporting material shall be provided to describe each of the following:

(1) The classes of subjects and objects controlled by the TCB. Examples of subjects are people, processes, or devices; and objects are records, blocks, pages, components, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc.

(2) How subjects are related to users.

(3) How subjects are assigned privileged conditions (trusted subjects).

(4) How users identify themselves to the TCB.

(5) How the TCB records events.

Block 10. PREPARATION INSTRUCTIONS (Continued)

10.4.2 Abstract mechanism segment. The actual model of the abstract TCB protection mechanism(s). Graphic representations of the model's segments may be included (e.g., diagrams and tables). These graphics may be annotated with English language descriptions. Supporting material shall be provided to describe each of the following:

a. All the rules that permit, as well as constrain, how a subject is allowed access to an object.
b. All privileged conditions under which certain kinds of subjects are allowed to bypass the identified mandatory and discretionary access control rules.
c. All controls on assigning privileged conditions to subjects.
d. All the controls on identifying users to the TCB.
e. All the rules that generate an audit event.
f. All TCB responses to failures.

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

10.4.3.1 General. There is no change to the general requirements of the Formal Security Policy Model document for TCB Class B1 products and their equivalent systems.

10.4.3.2 Policy segment. There is no change to the policy requirements of the Formal Security Policy Model document for TCB Class B1 products and their equivalent systems.

10.4.3.3 Abstract mechanism segment. The Formal Security Policy Model document shall identify the abstract TCB protection mechanism(s) and explain how these mechanisms satisfy the security policy model. Each abstract mechanism shall be discussed separately. Cross-reference these mechanisms to the policy portion of the Philosophy of Protection Report. The explanation shall include a description of how each element within a mechanism supports other elements of the mechanism, if any.

10.4.3.4 Segment integration. The integration of the policy and abstract mechanism segments of the model shall include the following:

a. An explanation to show that the formal security policy model is consistent with its axioms. The explanation shall provide rationale sufficient to demonstrate consistency.
b. A description of the relationship of each axiom to the model's segments and specific security-enforcement mechanism(s) in the model.
c. An explanation that shows that the TCB is sufficient to enforce the security policy. The explanation shall provide rationale sufficient to demonstrate consistency.

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

10.4.4.1 General. The TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in Class B1 TCBs to be extended to all subjects and objects.

Block 10. PREPARATION INSTRUCTIONS (Continued)

10.4.4.2 Policy segment. The Formal Security Policy Model document shall provide all theorems used in the model for each security policy segment, using both mathematical statements and an English language description. Supporting rationale for including the theorems shall be provided. The Formal Security Policy Model shall discuss how these theorems represent enforcement of the security policy.

10.4.4.3 Mechanisms segment The Formal Security Policy Model shall provide all theorems used in the model for the TCB protection mechanism(s), using both mathematical statements and an English language description. Supporting rationale for including the theorems shall be provided. The Formal Security Policy Model shall discuss how these theorems represent the TCB protection mechanism(s) and their enforcement of the security policy.

10.4.5 Segment integration. The Formal Security Policy Model document shall include an introduction to the kinds of proofs that are provided, along with a rationale that explains why these proofs are sufficient to demonstrate that the TCB is secure with respect to the security properties modeled. The integration of the policy and abstract mechanism segments of the model shall include the following proofs:

a. Proof that the model is consistent with its axioms, providing both the mathematical proofs and an English language description of the proofs.

b. Proof that shows that the TCB represented in the model is sufficient to enforce the security policy. The Formal Security Policy Model document shall trace each of the following:

(1) The security policy statements in the Philosophy of Protection Report to a formal mathematical statement. A cross reference matrix chart with detailed explanatory text may be used.

(2) The formal mathematical statements back to its security policy statements in the Philosophy of Protection Report. A cross reference matrix chart with detailed explanatory text may be used.

c. Proof for each of the theorems used in the model, both the mathematical proof and an English language description of the proof.