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 SECURITY FEATURES USER'S GUIDE	2. IDENTIFICATION NUMBER DI-MCCR-81349

3. DESCRIPTION/PURPOSE

3.1 The Security Features User's Guide informs users on how to make effective use of security features. It provides the necessary information to understand and effectively use the security protection mechanism(s) that secure processed or stored information.

4. APPROVAL DATE (YYMMDD) 930702	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) G/C71	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 2.2.4.1 and 3.2.2.1.1 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 user documentation for the security features as specified by DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria, Classes C1 (Discretionary Security Protection), and above, products or their equivalent systems. (Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER G6939

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 Security Features User's Guide 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 Features User's Guide.

g. Introduction. (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 and 10.4 is required for all class products and their equivalent systems applicable to the DID as a whole. In addition, the information required in 10.4.1 and 10.4.2 is necessary for various classes of products and their equivalent systems.

Block 10. PREPARATION INSTRUCTIONS (Continued)

h. Body of the Guide.
i. Attachments.
j. Appendices.
k. Bibliography. -List references and all applicable documents.
l. Subjective index. An exhaustive index of the key word or theme in each paragraph shall be provided.

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. The type font shall be 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 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 guide shall be provided in standard three ring notebook binders for ease of maintenance.

10.3 General The level of trust enforced by the Trusted Computing Base (TCB) shall determine the depth and size of the Security Features User's Guide (SFUG). This level determines the security functions needed. The SFUG shall describe the security functions used by operational users who are not specially trained as operators, security administrators, or system administrators.

10.4 Content. The SFUG shall be prepared as follows:

a. A description of the prominent features of each security protection mechanism(s) (e.g., I&A, DAC, MAC, and Object Manipulation Facilities) which pertain to the operational users shall be provided.

b. A description of the interface between the security protection mechanism(s) and the operational user. It shall also describe the use of the security protection features by the operational users. The SFUG shall include cautions and precautions concerning the consistent and effective use of the described protection features.

Block 10. PREPARATION INSTRUCTIONS (Continued)

c. The SFUG shall address the relationships between the operators, system administrators, or security administrators, and the operational user (e.g., the security administrator may control user password generation features). Interface(s) necessary for the user to understand his or her use of each security protection mechanism shall be completely described in the SFUG.

d. The SFUG shall include a description of expected reaction to security-related events (e.g., access violations, security- related failures). Every advisory or other response from each security protection mechanism(s) shall be documented, using the exact electronic text produced. Both affirmative and negative responses shall be illustrated by example dialogue (e.g., [User] Log-In Password Verified; [User] Access Denied; (User] Discretionary Permission Exceeded for File xxxx).

e. Cross-references to relevant documentation containing a more detailed description of the security protection mechanism(s) and their relationships shall be provided, where applicable, in the SFUG. All cross-references shall be to the subparagraph level in the referenced document.

f. Charts, figures, and caricatures should be used in the SFUG whenever possible to illustrate complex concepts, relationships, or interfaces to operational users not specially trained in security.

10.4.1 Class B2 products and their equivalent systems. The procedures for the operational user to utilize the trusted communication path between the TCB and the user for initial login and authentication shall be explicitly defined in the SFUG. The SFUG shall describe how the communications via this path is initiated exclusively by the user.

10.4.2 Class B3 and above products and their equivalent systems. The procedures for the operational user to utilize the trusted communication path between the TCB and the user for use when a positive TCB-to-user connection is required (e.g., login, change subject security level) shall be explicitly defined in the SFUG. The SFUG shall describe how the communications via this trusted path is activated exclusively by the user or the TCB. The SFUG shall describe how the trusted path is logically isolated and unmistakably distinguishable by the user from other paths.