DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

2. TITLE

COMMUNICATION SECURITY EQUIPMENT DESCRIPTION

1. IDENTIFICATION NUMBER

DI-MCCR-80339

3. DESCRIPTION / PURPOSE

3.1 The communication security (COMSEC) equipment description provides a description of a COMSEC equipment, device, or component; it describes in detail the equipment's functional, key and rekey, and transfer device interface design.

(Continued on Page 2)

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
870415	G/S4		

7. APPLICATION / INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated by the specific and discrete task requirement as delineated in the contract.

7.2 This DID is applicable to the development and acquisition of COMSEC equipment.

7.3 The requirements contained herein are applicable to all COMSEC equipment development, modification, and product improvement contracts.

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G4095

10. PREPARATION INSTRUCTIONS

10.1 General. This COMSEC equipment description will document in detail the COMSEC equipment's design to show that its design meets the Government Office of Key Managment's key architecture guidelines.

10.2 Content requirements. The COMSEC equipment description shall contain the following information:

10.2.1 Introductory Information. Introductory information shall state the purpose of the equipment, device, or component (i.e., encryption/decryption of teletype and data traffic).

10.2.2 Functional description. Defines the functional capabilities of the equipment, device, or component.

10.2.3 Compatible equipment list. Identifies and lists existing and/or developmental equipment that will have a compatible interface with this equipment, device, or component. Compatible fill/transfer devivces shall be included in this list. It shall also state how this (these) interface(s) was (were) verified.

10.2.4 Data rate. Defines all interface input and output data rates for this equipment, device, or component.

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

Block 3, Description/Purpose (Continued)

The principal uses of this DID are to provide the Government Office of Key Management input for equipment and/or system certification, and for determining equipment/system compatibility.

Block 10, Preparation Instructions (Continued)

10.2.5 Cryptonet size. Defines the cryptonet size for this equipment, device, or component. States whether this definition is proposed or approved, and if approved, identifies the approving authority.

10.2.6 Classification

10.2.6.1 Equipment. States the classification of this equipment, device, or component. Defines whether this classification applies to a keyed and/or unkeyed equipment, device, or component.

10.2.6.2 Data. Defines the highest classification level of data that can be stored and/or used in this equipment; device; or component.

10.2.7 Algorithm. Defines the algorithm(s) used in this equipment, device, or component. Identifies whether this (these) algorithm(s) has (have) been approved for use in this equipment, device, or component, or whether approval is pending. If approved, identifies the approving authority who approved the use of this (these) algorithm(s).

10.2.8 Cryptographic key. Defines the type(s), quantity(ies), size(s), bit pattern(s), cryptoperid(s), and storage capacity of cryptographic key proposed/approved for use in this equipment, device, or component. Identifies the approving authority for the application of this (these) key(s).

10.2.9 Rekey capability. Defines the method(s) (i.e., SAVILLE Advanced/Remote Keying (SARK), automatic remote rekeying, manual remote rekeying, key update capability) of rekey for this equipment, device, or component.

10.2.10 National Security Agency (NSA) Data Standard (DS) 100. Defines how DS-100 applies to and is used within this equipment, device, or component.

10.2.11 National Security Agency (NSA) Data Standard (DS) 101. Defines how DS-101 was incorporated within this equipment, device, or component.

10.2.12 Interface definition. Diagrams and defines all equipment interfaces. Specifies connectors and connector pins associated with key management functions (i.e., data input and output, rekey).

10.2.13 Timing diagram. Diagrams and defines internal equipment processes associated with key management functions (i.e., data processing, key generation, key translation, rekey).

10.2.14 Human interface. Separately specifies all operator actions and procedures associated with all key management functions (i.e., data processing, key generation, key translation, rekey). Defines operator actions in a step by step process.