DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

TITLE	1 IDENTIFICATION NUMBER
COMMUNICATION SECURITY SYSTEM DESCRIPTION	DI-MCCR-80340

3 DESCRIPTION / PURPOSE

3.1 The communication security (COMSEC) system description provides a description of a COMSEC system. It will describe in detail the COMSEC system's key management features.

3.1 The principle use of this description is to provide the Government Office of Key Management input for system certification.

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 a COMSEC system.

7.3 The requirements contained herein are applicable to all COMSEC system development, modification, and acquisition contracts.

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b AMSC NUMBER
		G4096

PREPARATION INSTRUCTIONS

10.1 General. This COMSEC system description documents in detail the COMSEC system's design to show that its design meets the Government Office of Key Management's key architecture guidelines.

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

10.2.1 Introductory information. States the purpose of this COMSEC system.

10.2.1.1 Communications architecture. Defines the communications requirements (voice, data, net size, net merging, etc.) for this COMSEC system.

10.2.1.2 Keying scheme. Defines the keying scheme (source, method of distribution, distribution medium, storage requirements, etc.) for this COMSEC system.

10.2.2 Net structure. Defines and graphically displays the net structure for this system, to include graphic displays of the net control stations, crypto net control stations, net controllers, etc.

10.2.3 Access control. Defines how, when, and where access control will be enforced to validate the need and authority to request, generate, handle, distribute store, and/or use cryptographic key within this COMSEC system.

(Continued on Page 2)

DISTRIBUTION STATEMENT

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

Block 10, Preparation Instructions (Continued)

10.2.4 Accounting. Defines how, when, and where accounting data will be collected, maintained, updated, transferred, and used to document cryptographic key generation, distribution, storage, use, and destruction within this COMSEC system. Differentiation must be described between automatic versus human action accounting initiated features.

10.2.5 Distribution. Defines how, when, and where cryptographic key will be distributed and translated to or within this COMSEC system.

10.2.5.1 Vulnerability. Defines how the contractor's distribution scheme will reduce the vulnerability to cryptographic key used within this COMSEC system.

10.2.5.2 Integrity. Defines how the distribution method(s) will assure the integrity of cryptographic key during the distribution process.

10.2.5.3 Identification. Defines how this COMSEC system will identify cryptographic key during its distribution.

10.2.6 Generation. Defines the key generation process by which cryptographic key is produced and specifies the algorithm(s), equipment, and/or system(s) they will support.

10.2.7 Recovery. Defines the recovery process by which secure communications can be restored after loss or compromise of cryptographic key. Differentiation must be described between automatic electrical distribution versus physical distribution recovery methods.

10.2.8 Request. Defines how the user will order cryptographic key for use within this system.

10.2.9 Storage. Defines how, when, and where the user will store cryptographic key within this COMSEC system.

10.2.9.1 Integrity. Defines how this/these storage method(s) will assure integrity of cryptographic key during storage.

10.2.9.2 Identification. Defines how this COMSEC system will identify cryptographic key during its storage.

10.2.9.3 Capacity. Defines this COMSEC system's capacity for cryptographic key storage.

10.2.10. Usage. Defines the use/function of each cryptographic key used within this COMSEC system (key encryption key, traffic encryption key, key production key, TRANSEC key, etc.).

10.2.10.1 Integrity. Defines how this COMSEC system will assure the integrity of cryptographic key during its use.

10.2.10.2 Identification. Defines how this COMSEC system will identify cryptographic key during its use.