DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

1 TITLE	2 IDENTIFICATION NUMBER
Preliminary System Security Concept (PSSC)	DI-MISC-80840

3 DESCRIPTION / PURPOSE

3.1 This Data Item Description outlines the format and content of the PSSC. The PSSC is a document which cites security concepts and requirements relative to a particular system. It is prepared by the contractor to provide the Government with preliminary description of security requirements and resources.

4 APPROVAL DATE (YYMMDD)	5 OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a DTIC APPLICABLE	6b GIDEP APPLICABLE
890605	AF 10	X	

7 APPLICATION / INTERRELATIONSHIP

7.1 This Data Item Description contains the format and content preparation instructions for data resulting from the work task described by 5.3.1.3 of MIL-STD-1785.

7.2 Security Vulnerability Analysis, DID DI-MISC-80841, is used with this Data Item Description when paragraphs 10.1.5.1 through 10.1.5.5 are cited.

7.3 Defense Technical Information Center (DTIC)
Cameron Station
Alexandria VA 22314-6100.

8 APPROVAL LIMITATION	9a APPLICABLE FORMS	9b AMSC NUMBER
		F4731

10 PREPARATION INSTRUCTIONS

10.1 The Preliminary System Security Concept (PSSC) shall include the following:

10.1.1 Program Data.

10.1.1.1 Title. Include the complete PSSC title.

10.1.1.2 Submitting Agency. List the name and address of the contract agency submitting the report and the name and telephone number of a project officer or point of contact.

10.1.1.3 Contract Citation. Identify the contract number and date as listed by the Government.

10.1.1.4 Security Tasks. Briefly describe major security tasks cited in the statement of work and related contract documents.

10.1.1.5 Distribution. List the name and address of Government and contract agencies receiving copies of this concept. If necessary list them in an appendix and make reference to it here.

10.1.2. System Concept.

(Continued on Page 2)

11 DISTRIBUTION STATEMENT

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

Block 10, Preparations Instructions (Continued)

10.1.2.1 Description. Briefly describe the system and its major components. Cite separate configurations for initial operational capability (IOC) and full operational capability (FOC), if different.

10.1.2.2 Performance requirements. Cite the major performance and deployment criteria listed in the applicable statements of work and other related contract documents which affect security.

10.1.2.3 Reliability and Maintainability. Identify security issues affecting system reliability, logistics reliability, availability, and maintainability.

10.1.2.4 System Survivability. Show self-protection capabilities or subsystem designs which may enhance security (Examples include devices against tampering and spoofing, chemical or biological radiation hardness, nuclear hardness, nuclear and non-nuclear electromagnetic pulse hardness, and use of passive detection technology.)

10.1.2.5 Preplanned Product Improvements (P3I). Describe provisions or security implications for subsystem growth or improvements such as modifications and upgrades.

10.1.3. Security Subsystem Employment Data.

10.1.3.1 General employment description. Describe how, where, when and what security subsystems will be used and how they will be integrated with the system(s) they support.

10.1.3.2 Command and control structure. Describe the command and control data that must be exchanged. Explain how security subsystems will be integrated into the command and control structure projected to exist when it is deployed.

10.1.3.3 Information systems. Identify other information that must be exchanged between this subsystem and other systems, subsystems or components. Cite the expected length of each communications link, anticipated flow rate across each link, required availability of each link, etc.

10.1.3.4 Security subsystem standardization, interoperability, and commonality. Describe requirements for joint service interface, NATO cross-servicing and interoperability with existing systems or subsystems. Identify procedural and technical interface standards incorporated in subsystem design.

10.1.3.5 Operational environment. Describe climatic and atmospheric environmental effects and considerations. If applicable, define the chemical and biological environment in which equipment must function.

Block 10, Preparation Instructions (Continued)

10.1.4. Security Subsystem Support.

10.1.4.1 Maintenance planning. Outline the actions, support, and documentation necessary to establish maintenance concepts and requirements. Include maintenance tasks to be accomplished for on- and off-equipment maintenance; interservice, organic and contractor mix, workloads, and time phasing for depot maintenance. Explain the management strategies for selecting and integrating contractor and government furnished equipment.

10.1.4.2 Manpower and personnel. Outline the projected manpower requirements envisioned to support this subsystem(s). Include type of specialty codes and skill levels required, time phased reporting, etc.

10.1.4.3 Supply support. Show the proposed approach for provisioning initial support and acquiring, distributing, and replenishing inventory spares and repair parts.

10.1.4.4 Support equipment. Identify equipment required to support this subsystem(s). Include ground handling and maintenance equipment, tools, metrology and calibration equipment, and related computer hardware and software.

10.1.4.5 Training and training devices. Describe the training support concept from security subsystem design through deployment. Identify the command or agency responsible for developing and conducting each phase of training. Show inventory items and training devices by projected type, number, use, and locations required. Outline initial and recurring training requirements by location, type, specialty, and fiscal year.

10.1.4.6 Computer resources support. Define special computer program documentation, related software, source data, facilities, hardware, etc. required for subsystem support.

10.1.4.7 Facilities. Specify facility, shelter and housing external to system-designed survivability features.

10.1.4.8 Packaging, handling, storage and transportation. Describe the requirements, resources, processes, procedures, design considerations, and methods to ensure security subsystems are properly preserved, packaged, handled, and transported.

10.1.4.9 Related support factors. Describe those pertinent support factors, considerations or requirements not covered elsewhere, but deemed important to the effectiveness of the security subsystem.

10.1.5. General Provisions for System Security. Address the following security issues relative to overall system deployment and operation.

Block 10, Preparation Instructions (Continued)

10.1.5.1 Threat assessment. Address security threats to the system for design, development, production, at IOC and throughout its projected life. Include foreign government capabilities, peace and wartime ground threats, and system-unique vulnerabilities. Make reference to government threat documents. In addition, cite requirements for threat analysis and security vulnerability assessments.

10.1.5.2 Procedural requirements. Cite security force and procedural requirements which apply to pre-, trans-, and post-attack operations in support of the Air force Physical Security Program.

10.1.5.3 Security resources. Cite security manpower, facility and equipment requirements in the quantities, type, and configuration necessary to support the system when deployed.

10.1.5.4 Security response planning. Address emergency security response planning, which reflects the general design of the security force posture calculated to produce the greatest invulnerability to terrorism, sabotage, overt and covert attack. It is supported by the threat and vulnerability assessments cited in 10.1.5.1. In addition, briefly describe how a security reporting and alerting system will be implemented.

10.1.5.5 Security priorities for all applicable systems and components. Include security priorities for all operational phases, including maintenance. For example, aircraft system priorities would include nuclear alert, nonnuclear alert, mission capable and nonalert. In addition, explain how waivers, exceptions, and variances to security criteria will be identified, submitted, approved, and corrected.

10.1.5.6 Security requirements from related security disciplines. Include applicable information security, physical security, computer security personnel security, product security, industrial security, operations security, communications security, electronic security, survivability, antiterrorism and counter-intelligence aspects.

10.1.5.7 Facility and equipment requirements. Facility and equipment requirements which are incorporated into the system to support system security requirements. These requirements include:

a. The Central Security Control Facility, Master Surveillance and Control Facility, Security Force Response Facility, entry control facilities, etc.

b. Barrier systems and warning signs.

c. Alarm annunciation and display equipment.

d. Security force armament and duty equipment.

e. Security force communications. Include fixed, portable and landline requirements by type and number.

f. Interior and exterior intrusion detection systems.

Block 10, Preparation Instructions (Continued)

10.1.5.8 Manpower standard. Identifies security force post and patrol requirements for normal operations.

10.1.5.9 Security force logistics. Cite security force logistics and materiel requirements including vehicles and associated equipment, special purpose equipment, training aids, tool kits, new armament, etc.

10.1.5.10 Entry access controls. Include system entry control requirements for all restricted areas including:

a. General criteria and unique requirements for entry control. Include the rate at which individuals must be processed during normal operations, alert operations, and periods of advanced readiness.

b. Qualification requirements for the various categories of people who must enter.

c. Personnel clearance and investigative requirements.

d. Special training or briefing and debriefing requirements.

e. Authentication and duress code techniques and procedures.

f. Dispatch control procedures for unattended or minimally staffed sites.

g. Description of the badge system, emergency procedures, and personnel escort requirements; including the number of individual names maintained in entry data files.

☆U.S. GOVERNMENT PRINTING OFFICE: 1989 - 604-032/00073