DATA ITEM DESCRIPTION

Form Approved
OMB No 0704-0188

1. TITLE
OPERATIONS SECURITY (OPSEC) PLAN

2. IDENTIFICATION NUMBER
DI-MGMT-80934

3. DESCRIPTION/PURPOSE

3.1 The OPSEC Plan describes the methods to: (1) Identify OPSEC security responsibilities and requirements, (2) Define overall OPSEC security standard practice procedures, (3) Identify potential problem areas and determine solutions, and (4) Develop OPSEC security awareness inputs into the overall system security process. (Continued on Page 2)

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
900125	A/CSSD-BM		

7. APPLICATION/INTERRELATIONSHIP

7.1 This DID contains the format and content preparation instructions for the data product generated by the specific and discrete task requirements delineated in the contract.

7.2 The DID is applicable only when the contracting activity determines that the sensitivity of the contract warrants the effort.
(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		A4877

10. PREPARATION INSTRUCTIONS

10.1 Reference documents. The applicable issue of the document cited herein, including their approval dates and dates of any applicable amendments, notices and revisions shall be as specified in the contract.

10.2 Format. The OPSEC Plan format shall be contractor selected. Unless effective presentation would be degraded the initially used format arrangement shall be used for all subsequent submissions.

10.3 Content. The OPSEC Plan shall contain the information required by the guidelines of Sections 2, 3, and 4 of the Industrial Operations Security (OPSEC) Guide to include the results of the four-step OPSEC analysis described therein including those aspects of the hostile intelligence threat that are applicable to the specific contract.

10.3.1 General. The OPSEC Plan shall contain details of the OPSEC management concept to include contract identification, assignment of responsibilities, definition of milestones with target dates, provisions for continuous analysis, and periodic revision as the contract activities evolve and become more specific and detailed.
(Continued on Page 2)

DISTRIBUTION STATEMENT

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

Block 3. Description/Purpose (Continued)

3.2 The Plan is utilized to identify and monitor a contractor's OPSEC activities during performance of the contract.

Block 7. Application/Interrelationship (Continued)

7.3 The initial submission may be broad in scope; however, the level of detail increases as the work progresses to the point that any security-related question will be addressed in the Plan.

7.4 The contractor's implementation of the OPSEC Plan, approved by the contracting activity, is also subject to joint inspection by the Defense Investigative Service and the contracting activity.

7.5 The Industrial Operations Security (OPSEC) Guide is available from U. S. Army Strategic Defense Systems Command, P.O. Box 1500, Huntsville, AL 35807-3801.

7.6 This DID supersedes DI-A-1022.

Block 10. Preparation Instructions (Continued)

10.3.2 Threat. The OPSEC Plan shall contain the threat provided by the contracting activity and include only that portion deemed applicable to the specific contract activities.

10.3.3 Sensitive Aspects of the Contract. The OPSEC Plan shall contain an overview of all activities, operations, tests, etc. to be undertaken in performance of the contract; identify those in which classified information will manifest itself; identify the topics of the classification guide that specify the information is classified; determine how, where, and when the classified information is embodied in the hardware, software, or operations; determine what type access (visual, physical possession, etc.) permits knowledge of the classified information, what tools/equipment/capability are required, and the specific national defense advantage provided by the information if it is protected. Use of electro-mechanical equipment is an operation that shall be included, as are subcontracting, hardware-in-the-loop testing, calibration and check-out, fabrication, static tests, breadboard and brassboard fabrication and

(Continued on Page 3)

Block 10. Preparation Instructions (Continued)

testing, laboratory experiments, etc. Based on the above analysis, an Essential Elements of Friendly Information (EFFI) List shall be prepared. This list is to include all the information considered "essential" to the success of the effort, all the information that must be protected to preserve the military advantage potentially provided by the effort. Additionally, the list shall include all the activities, operations, tests etc. that could reveal the "essential" information to hostile intelligence.

10.3.4 Vulnerabilities. The OPSEC Plan shall contain vulnerabilities derived by comparing threat to sensitive activities to determine which sensitive activities can be observed by hostile intelligence. "Observe" is defined to include all physical and chemical properties that can be noted and recorded by any type sensor. One such property is unintentional electromagnetic emanations which may convey classified information. On this basis, TEMPEST is a part of OPSEC, and the instructions in the Industrial OPSEC Guide shall be followed to identify potential TEMPEST vulnerabilities.

10.3.5 Countermeasures. The OPSEC Plan shall, for each vulnerability, include the protective measure deemed appropriate to negate or reduce the potential damage to the project.