DATA ITEM DESCRIPTION

Title: OPERATIONS SECURITY (OPSEC) PLAN

Number: DI-MGMT-80934A
AMSC Number: N7553
DTIC Applicable: No
Office of Primary Responsibility: N/AIR-7.4
Applicable Forms: N/A

Approval Date: 20050406
Limitation: N/A
GIDEP Applicable: No

Use/relationship: The OPSEC Plan is used to identify and monitor a contractor's OPSEC activities during performance of the contract. 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.

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

b. This DID is applicable only when the contracting activity determines that the sensitivity of the contract warrants the effort.

c. 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 OPSEC Plan.

d. 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.

e. This DID supersedes DI-MGMT-80934.

Requirements:

1. Reference documents.

a. Applying OPSEC to U.S. Government Contracts Pamphlet (available from the Interagency OPSEC Support Staff, ATTN: Product Distribution Officer, 6411 Ivy Lane, Suite 400, Greenbelt, MD 20770-1405)

b. 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.

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

3. Content. The OPSEC Plan shall contain the information required by the guidelines of the Applying OPSEC to U.S. Government Contracts Pamphlet to include the results of the five-step OPSEC analysis described therein including those aspects of the foreign intelligence threat that are applicable to the specific contract.

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.

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.

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 that information if it is protected. Use of electromechanical 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 testing, laboratory experiments, etc. Based on the above analysis, a list of critical information shall be prepared. This list is to include all the information considered essential to the success of the effort, and 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 “critical” information to foreign intelligence.

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 foreign 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 guidelines in the Applying OPSEC to U.S. Government Contracts Pamphlet shall be followed to identify potential TEMPEST vulnerabilities.

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.

4. END OF DI-MGMT-80934A