DATA ITEM DESCRIPTION

Title: NAVAIR OPERATIONS SECURITY (OPSEC) PLAN

Number: DI-MGMT-81999
AMSC NUMBER: 9593
DTIC Applicable:
Preparing Activity: AS
Applicable Forms:

Approval Date: 20151013
Limitation:
GIDEP Applicable:
Project Number: MGMT-2015-019

Use/Relationship: The OPSEC Plan is used to identify and monitor a contractor's OPSEC activities during the performance of a contract. It is intended to be a living document that will require periodic updates throughout the life of the contract. The OPSEC plan; (1) Describes the OPSEC environment to include identification of critical information, the OPSEC threat and vulnerabilities an adversary might exploit to acquire critical information, (2) Documents the OPSEC risk analysis, (3) Identifies proposed and actual OPSEC measures, (4) Defines and assigns specific OPSEC responsibilities and ties the OPSEC Plan to the contractor's corporate OPSEC Program, and (5) Serves as a repository of the OPSEC history of the contract.

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.

This DID is applicable only when the contracting activity determines that the sensitivity of the contracted effort warrants OPSEC protections.

The contractor's implementation of the OPSEC Plan, approved by the contracting activity, is subject to joint audit and/or inspection by the Defense Security Service and the contracting activity.

Requirements:

1. Reference documents. The content of this DID shall identify changes as specified in the following:

a. Title 15, US Code, Section 278g-3(d)(4). Use the definition of sensitive information.

b. DOD Manual 5220.22.M. "National Industrial Security Program Operating Manual (NISPOM)"

c. OPNAVINST 3432.1 Department of the Navy Operations Security Program

d. OPNAVINST 3432.1A Operations Security dated 4 Aug 2011

e. National Security Decision Directive 298 of 22 January 1988. Use for concept of Operations Security, and apply the framework for telecommunications security in DFARS clause 252.239-7016, as appropriate.

2. Format. The OPSEC Security Plans shall be submitted in contractor determined format.

3. Content. The content of this plan shall consist of the following:

3.1 COVER PAGE

The cover page for an OPSEC Plan shall clearly present the following information:
1. Title of the Acquisition Program
2. Title of the Document (i.e. “Operations Security Plan”)
3. Reference to the government contract number
4. Date of latest revision
5. Name, signature and title of the preparer of the OPSEC Plan
6. Name, signature and title of the approver of the OPSEC Plan.
7. Reference for whom the document was prepared (Contracting activity)
8. Reference by whom the document was prepared (Corporation)
9. All appropriate distribution or classification statements

3.2 TABLE OF CONTENTS PAGE

The Table of Contents for an OPSEC Plan shall outline each section contained in the OPSEC Plan.

3.3 PREFACE PAGE

The purpose of the Preface is to provide a brief, unclassified, overview of the program and the need for OPSEC measures. The specific objectives of the contracted effort shall be introduced with reference to all strategic participants and partnerships required to make the program a success. The anticipated development of any innovative concepts or technologies shall also be introduced in the Preface.

The Preface shall reference all links between the OPSEC Plan and any corporate OPSEC Program(s). The Preface may conclude by referencing requirement documents such as the contract number, Contract Security Classification Specification (DD254), Contract Data Requirements List (DD1423) and any other pertinent guidance provided by the contracting activity. It shall also provide an OPSEC point of contact, with contact information, for additional guidance or assistance such as the OPSEC program manager or contractor program manager.

3.4 OPSEC PLAN INTRODUCTION

3.4.1 Purpose and Scope: The purpose of the OPSEC Plan shall be effectively communicated in this section and include a description of the scope of the OPSEC Plan (unique physical locations, subcontractors, suppliers, period of performance, etc.).

3.4.2 Authorities: The requirement to protect critical information shall be documented within this section. Documenting the requirement can be achieved by referencing the Corporate OPSEC Program (Policy) and Plan, DODM 5205.-2M, specific contract documents including the DD254 for contracts involving classified data, or other contracting activity specific guidance.

3.4.3 OPSEC Plan Major Activity Timeline: This section shall include a list of all

major OPSEC Plan activities such as quarterly OPSEC Working Group Meetings, Annual Assessments, scheduled OPSEC awareness training, Sub-contractor OPSEC Assessments and Surveys, Threat and Vulnerability Reviews, etc. This section shall also include scheduled OPSEC Plan reviews.

3.4.4 Responsibilities: The OPSEC Plan shall identify whom is responsible for the major activities described in the Plan. For example (not intended as an inclusive list):

The OPSEC Manager shall be identified by name and include a list of duties that may include:

1. Coordinate all OPSEC policy responsibilities/ procedures within the program.
2. Revise the Program OPSEC Plan as necessary.
3. Convene and coordinate the annual Program OPSEC Assessment.
4. Disseminate updated threat information to program personnel.
5. Assist in the review of contract requirements for OPSEC considerations.
6. Conduct OPSEC briefing(s) upon customer approval of the plan.
7. Principal advisor to the Contractor Program Manager on all OPSEC matters.
8. Develop/Disseminate Program Critical Information List (CIL).
9. Promote OPSEC awareness within the program.

The Contractor Program Manager shall be identified by name and include a list of duties that may include:

1. Responsible for the overall implementation of the program/contract.
2. Ensure proper OPSEC procedures are implemented by program personnel.
3. Ensure all subcontractors and suppliers supporting the program develop and implement procedures in compliance with the Program OPSEC Plan.
4. Remain cognizant of emerging OPSEC threats and vulnerabilities that may adversely impact upon the success of the program.
5. Actively participate in periodic Program OPSEC assessments.
6. Remain cognizant of any changes in critical information and communicate them to the Program OPSEC Manager.
7. Promote OPSEC awareness within the program.

A short description of the expectations and responsibilities of all program personnel (including subcontractors and suppliers) shall be provided and may typically include:

1. Remain compliant with all applicable OPSEC Plans.
2. Maintain an awareness of all applicable CIL.
3. Attend all OPSEC program briefings.
4. Timely reporting of any OPSEC concerns to the Contractor Program Manager and/or the Program OPSEC Manager.
5. Generation of OPSEC Plans (sub-contractors or suppliers only).

3.4.5 Organizational OPSEC Communications and Interfaces: A description as to how the OPSEC Plan will be communicated to all personnel supporting the program (hardcopy, via a webpage, briefings, etc.).

3.4.5.1 Internal: In this section the OPSEC Plan shall identify all anticipated OPSEC interfaces internal to the corporation such as the senior corporate leadership, corporate OPSEC Working Group, OPSEC coordinators, program personnel, etc.

3.4.5.2 External: In this section the OPSEC Plan shall identify all anticipated external points of contact such as the contracting activity, Defense Contract Management Agency (DCMA), The Defense Security Service (DSS), Federal Bureau of Investigation (FBI) and local law enforcement and their primary role within the OPSEC program (i.e. DCMA audits acquisition management practices, DSS provides security oversight, FBI and law enforcement may provide threat data). Subcontractor and supplier OPSEC points of contact shall be similarly identified.

3.4.6 Marking, Handling and Distribution of Documents: This section shall provide a description of marking, handling, storage, access and transmission authorizations and procedures for any critical information provided to, or generated by, the contractor.

Reference to the program classification guide, Freedom of Information Act and any additional guidance provided by the contracting activity may be cited as applicable.

3.5 THREAT

3.5.1 General Threat: This section shall identify and demonstrate an understanding of the overall threat to program critical information throughout the anticipated duration of the contract/program. For example, an information systems program might note the following:

> DSS analysis of 2008 threat data shows, "Information systems, especially C4ISR related systems remained the primary sought-after technology for East Asia and Pacific Region countries. Direct requests (often via the Internet) and other suspicious Internet activity continued to be the preferred method of collection. Information systems are primary targets for Near East adversaries of the United States. Near East commercial entity activity indicates a growing collusion between commercial entities and government associated entities such as universities, public agencies and research and development centers. Adversaries using HUMINT and OSINT collection methods represent a significant threat to program critical information.

The section shall conclude with a brief description of all identified intelligence collection methods that may be expected to be used by an adversary to acquire critical information.

Note: A general description of intelligence collection methods may be found in "Applying OPSEC to Government Acquisitions and Contracts" at www.ioss.gov.

3.5.2 Program Detailed Threat: This section shall be similar to section 3.5.1 above referencing any known direct threats to acquisition specific elements of critical information within the

program/contract. As complete a description of each threat as possible shall be provided while maintaining the overall plan classification at the unclassified level. Since detailed threat information may derive from classified sources, reference to source documents as provided by the government contracting activity or other reputable source is permitted.

3.5.3 Threat Analysis: Each threat identified in sections 3.5.1 and 3.5.2 shall be analyzed to determine the level of threat to the corresponding critical information. The results of this analysis shall be presented in this section. A description of the specific threat analysis method used by the contractor to quantify each threat shall be included in this section.
Note: For additional guidance and a sample threat analysis methodology see, "Applying OPSEC to Government Acquisitions and Contracts" at www.ioss.gov and DODM 5205.02.

3.5.4 Changes Within Threat Environment: The Threat section shall conclude with a statement that addresses how new threat data is to be received and incorporated into the OPSEC Plan to ensure OPSEC risk remains in compliance with all applicable guidance.

3.6 CRITICAL INFORMATION

3.6.1 General: Critical information shall be identified within this section of the plan and a comprehensive program Critical Information List (CIL) shall be included.

3.6.2 Critical Information List: Guidance on the creation of a CIL is contained within "Applying OPSEC to Government Acquisitions and Contracts," available at www.ioss.gov, DODM 5205.02M, or may be provided by the contracting activity. Ideally the CIL shall remain unclassified to facilitate wide internal distribution, but may provide reference to classified information as applicable.

3.7 VULNERABILITY

3.7.1 General: The Vulnerability section of the OPSEC Plan shall describe the analysis of activities (indicators) that point to OPSEC vulnerabilities an adversary can exploit to acquire critical information. This section shall contain a list of all identified OPSEC vulnerabilities.

3.7.2 List of OPSEC Vulnerabilities: Each vulnerability shall be described in sufficient detail as to communicate to the contracting activity the extent of the vulnerability. The Vulnerability List shall remain unclassified, but may provide reference to classified information if applicable. Reference to classified reports and other information shall include an unclassified description of the documentation (report title, number, etc.) and the source responsible for publication of the information.

Note: A list of typical OPSEC vulnerabilities which may require OPSEC measures may be found within "Applying OPSEC to Government Acquisitions and Contracts", available at www.ioss.gov or may be provided by the contracting activity. These sample vulnerabilities are not all inclusive and the submitted vulnerability list shall be tailored to the specific acquisition or contract.

3.7.3 Vulnerability Analysis: Once potential program vulnerabilities have been identified, the magnitude of each vulnerability shall be determined using a consistent methodology identified and documented in this section of the OPSEC Plan. The results of this analysis shall also be described in this section.

Note: For additional guidance and a sample vulnerability methodology see, "Applying OPSEC to Government Acquisitions and Contracts" at www.ioss.gov and DODM 5205.0-2M.

3.8 RISK ASSESSMENT

3.8.1 General: The OPSEC risk of a program represents the probability of compromise of critical information and the impact to the program/contract taking into account the threat and vulnerabilities. The acceptable level of OPSEC risk (as determined by senior leadership, or the contracting activity) shall be described in this section in terms consistent with the selected OPSEC methodology.

3.8.2 Risk Assessment: The specific OPSEC risk shall be described in terms consistent with the OPSEC methodology selected for determining OPSEC threat and vulnerability. The method, and the results of the assessment, shall be presented in this section. The conclusion of the risk assessment shall result in an ordinal ranking of OPSEC risk (highest to lowest).

Note: Additional guidance and a sample risk methodology are available in "Applying OPSEC to Government Acquisitions and Contracts" at www.ioss.gov and DODM 5205.0-2M.

3.9 OPSEC MEASURES

3.9.1 General: This section of the OPSEC Plan shall identify specific OPSEC Measures proposed for mitigating OPSEC risk to acceptable levels including the cost to implement each measure. A sampling of common OPSEC measures is available in "Applying OPSEC to Government Acquisitions and Contracts" at www.ioss.gov. This list is not to be considered exhaustive and is provided as guidance for the development of the program/contract specific list of potential OPSEC measures.

3.9.2 Residual Risk: This section shall contain an analysis of residual OPSEC risk, in terms consistent with the OPSEC methodology selected, as a result of implementation of each OPSEC measure presented in section 3.9.1. This section shall identify which OPSEC measures will be implemented and the rationale for those that will not.

3.10 OPSEC Program Chronology: This section shall document significant program OSPEC events throughout the lifecycle of the program. Significant events may include changes to the CIL, changes in program leadership or results of program assessments and surveys (including subcontractors). At a minimum, this section shall include a brief description of the event, date of occurrence, actions taken by the contractor and final disposition. A known compromise of critical information need only be referenced in keeping with the intended classification of this document.

Note: The history contained herein may be used by the government as a part of an OPSEC or security audit conducted by the contracting activity, DSS or other authorized agency.

3.11 ACRONYMS: This section shall include a complete list of acronyms used in the Program OPSEC Plan (i.e., CDRL – Contract Data Requirements List, DID – Data Item Description, etc.).

3.12 REFERENCES: This section shall include a complete list of all references cited in the Program OPSEC Plan (i.e. DoD Manual 5205.02-M, dated November 3, 2008, Contract Number, Corporate OPSEC Plan(s)/Program(s), etc.).
The specific example provided derives from annual documentation produced by the Defense Security Service, Counterintelligence Office in 2009. Current assessments may be found at https://www.dss.mil/isp/count_intell/count_intell.html.

End of: DI-MGMT-81999