TITLE OF PROGRAM

OPERATIONS SECURITY PLAN

Contract No. _____

Date

Prepared by: _____(signature)_____ Approved by:_____(signature)_____
Typed Name **Typed Name**
Title **(Pres/CEO/Head of Co., etc.)**
Title

Prepared for:
Contracting Organization
Address

Submitted by:
Contractor
Address

Controlled by: **[Name of DoD Component] (Only if not on letterhead)]**
Controlled by: **[Name of Office]**
CUI Category: **[List category or categories of CUI]**
Distribution/Dissemination Control: **[B, C, D, E, or F / FEDCON]**
POC: **[Phone or email address]**

(WHEN COMPLETED need this notice)
NOTICE: Do not publicly disseminate sensitive information. Any further dissemination without authorization from JMC is prohibited. Personnel who fail to protect sensitive information from unauthorized disclosure may be subject to administrative, disciplinary, contractual, or criminal action.

TABLE OF CONTENTS

SAMPLE

1. General 4
1.1 Administration
1.2 Applicability
1.3 Responsibilities
1.3.1 OPSEC Coordinator
1.3.2 Personnel
1.4 Purpose
1.5 Subcontractor Applicability
1.6 Controlled Unclassified Information (CUI)
1.6.1 Handling, Storing & Transmitting CUI
1.6.2 Markings
1.7 Distribution Requirements for Technical Documents
1.7.1 Distribution Statement Definition
1.7.2 Handling and Destroying Limited Distribution Documents
1.7.3 Export Control Warnings
2. Critical Information 8
3. Threats 8
3.1 General Applicability
3.2 Human Intelligence (HUMINT)
3.2.1 Overt – Open Source Intelligence (OSINT)
3.2.2 Visitors
3.2.3 Covert – Illegal Entry/Coercion/Collusion
3.3 Signals Intelligence (SIGINT)
3.4 Imagery Intelligence (IMINT)
3.5 Measurement & Signatures Intelligence (MASINT)
3.6 Intelligence Threats to (**company**)
3.6.1 Worldwide General Threat
3.6.2 Changing Nature of the Worldwide Threat
3.6.3 Intelligence Collection Threat to (**company)**
4. Vulnerabilities 12
4.1 General Vulnerabilities
4.2 Contractual Vulnerabilities
5. Assessment of Risk 13
6. OPSEC Measures 13
5.1 General OPSEC Measures
5.2 Contractual OPSEC Measures
7. Self-Assessment 15
8. Training Awareness 15
8.1 General
8.2 Initial OPSEC Training/Orientation
8.3 Refresher Training
8.4 OPSEC Awareness

SAMPLE

8.5 Training of Designated OPSEC Officials
8.6 OPSEC Training Resources
8.7 CUI
8.8 CUI Awareness
8.9 CUI Training Resources

ACRONYMS 15
REFERENCES 15

SAMPLE

1. GENERAL

1.1 ADMINISTRATIVE

This Operations Security (OPSEC) Plan will serve as the implementing document for contract activities undertaken by **(company name)** on the **(program name)** program under **(contract number)**. The specific objectives of this contractual effort are to **(produce… what?)**. A copy of the plan will be available for each participant to review. This plan will be reviewed periodically by the OPSEC Coordinator as additional intelligence threat information becomes available, or as the program plan changes, but no less than annually. Specific changes may be required periodically by the JMC, or as OPSEC considerations on this program occur.

1.2 APPLICABILITY

This plan is applicable to appropriate **(product name)** elements at all **(company name)** and subcontractor facilities and locations that may be tasked to work on the program. Each subcontractor is responsible for OPSEC implementation. **(Add additional information as necessary)**.

1.3 RESPONSIBILITIES

1.3.1 OPSEC COORDINATOR

The **(company name)** OPSEC Coordinator is responsible for developing the OPSEC Plan and monitoring its implementation and operation to ensure compliance. He serves as the principal advisor to the **(company name)** on all OPSEC matters and will:

1) Coordinate all OPSEC policy responsibilities and procedures within the program.
2) Revise the OPSEC Plan as necessary.
3) Coordinate the annual review and update of the sensitive aspects of the program.
4) Accumulate and disseminate updated threat information to program personnel.
5) Assist in the review of contract requirements for OPSEC considerations.
6) Conduct OPSEC Program briefing(s) after customer approval of the plan.
7) Ensure that all other facilities supporting the program develop similar procedures or comply with the requirements of this plan.

1.3.2 PERSONNEL

Employees associated with **(program name)** are required to attend all Program OPSEC briefings. Personnel must comply with all OPSEC principles and procedures. Program personnel should consider this OPSEC Plan as their plan to protect the U.S. technological lead and **(company name)**'s competitive position. How well each team member protects

SAMPLE

sensitive information on this project may not only affect our national security but may directly impact **(company name)**'s future business endeavors.

1.4 PURPOSE

The five steps in the OPSEC cycle are:

1) Identification of Critical Information,
2) Analysis of threats,
3) Analysis of vulnerabilities,
4) Assessment of risk, and
5) Application of OPSEC measures.

The five-step cycle is continuous and assessment should occur frequently throughout the operation. OPSEC is a mandated program designed to safeguard sensitive program information, operations and activities which if exploited could compromise current or future plans and activities. This is accomplished by the identification and elimination or control of vulnerabilities that might be exploited by intelligence analysis. This OPSEC plan is designed to document the OPSEC analysis and outline procedures to be followed by program employees to prevent the disclosure of classified information and/or minimize revelation of sensitive information, activities, and operations to any unauthorized person, thus purposefully impeding intelligence collection efforts. Applicable activities and operations of the contract will be analyzed to determine known or suspected vulnerabilities to this program. Countermeasures designed to eliminate or reduce these vulnerabilities to an acceptable risk level have been established and implementing instructions are identified in Section 6 of this plan.

1.5 SUBCONTRACTOR APPLICABILITY

OPSEC will apply to the activities of **(subcontractor names)**. They must implement and operate within the approved **(company name)** OPSEC Plan. An OPSEC assessment of their activities must be conducted, documented and submitted to **(company name**) for approval. International subcontractors, as well as any additional U.S. subcontractors, will receive OPSEC guidance, as applicable. Determination as to whether OPSEC should be imposed is the responsibility of each subcontractor with respect to his or her lower tier suppliers in accordance with the guidance received from its prime contractor. For those subcontractors not conversant or experienced with the Operations Security Program, **(company name**) will provide additional guidance to aid in the development of their OPSEC Plan.

1.6 CONTROLLED UNCLASSIFIED INFORMATION (CUI)

(Company name) has been authorized to receive, generate, and protect CUI material as part of the Contract Requirements. This section outlines the requirements for safeguarding CUI. CUI includes topics of unclassified information that are eligible for

SAMPLE

exemption from mandatory public disclosure under the Freedom of Information Act (FOIA). **(Company name)** is also authorized to protect as CUI, information that is:

1) Contained in commercial or financial information generated by or for the Government with the understanding it is on a privileged or confidential basis (e.g., bids, contracts, proposals, trade secrets, inventions, discoveries, proprietary data, or data on contract performance, income, profits, losses and expenditures, etc.).

2) Included in communications to Government agencies and Commands that offer advice, suggestions, or reports prepared on behalf of the Army; and received or generated by a Command preliminary to a decision or action where premature disclosure would interfere with the purpose for which the records are created.

1.6.1 HANDLING, STORING, AND TRANSMITTING CUI

Program personnel shall be briefed on CUI procedures. Access to CUI material will be limited to those personnel who need the material to do their job. CUI material shall be handled in a way to preclude its disclosure to the general public. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. After working hours, CUI information will be stored in locked desks, file cabinets, bookcases or similar items. CUI documents can be transmitted via first class mail, parcel post, or, for bulk shipments, fourth class mail. Electronic transmission of CUI information by voice, data, facsimile or similar means, should be by approved secure communications systems whenever possible. CUI documents will be disposed of by shredding or tearing into pieces and discarding the pieces in regular trash containers.

1.6.2 MARKINGS

All materials defined as Controlled Unclassified Information will be marked “CUI” in letters larger than the rest of the text near the bottom of each unclassified page. Program personnel will contact the OPSEC Coordinator to receive instruction on proper markings.

1.7 DISTRIBUTION REQUIREMENTS FOR TECHNICAL DOCUMENTS

All technical documents, including such informal documents as working papers, memoranda, and preliminary reports if those documents are not already in the public domain, and if they are likely to be disseminated outside of the Department of Defense shall be marked with the appropriate distribution statement. Technical information is defined by DoD Instruction 5230.24 as: information, including scientific information, that relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment. Distribution marking requirements apply to technical information generated in any form.

1.7.1 DISTRIBUTION STATEMENT DEFINITION

SAMPLE

A statement used in marking a technical document to denote the extent of its availability for distribution, release, and disclosure without additional approvals or authorizations. A distribution statement marking is distinct from, and in addition to, a security classification marking assigned in accordance with DoD Instruction (DoDI) 5200.01 (Reference (b), Provides procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP).

Distribution statements and notices authorized for use on DoD technical documents to limit their distribution as well as the reasons and definitions for such markings can be found in DoD Instruction 5230.24, Distribution Statements on Technical Documents, 10 January 2023.

1) DISTRIBUTION A – Approved for public release. Distribution is unlimited."
2) DISTRIBUTION B – Distribution authorized to U.S. Government agencies only (fill in reason) (date of determination or this document shall be referred to (insert controlling DoD office)."
3) DISTRIBUTION C – Distribution authorized to U.S. Government agencies and their contractors (fill in reason) (date of determination). Other request for this document shall be referred to (insert controlling DoD office)."
4) DISTRIBUTION D – Distribution authorized to the Department of Defense and U.S. DoD contractors only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office)."
5) DISTRIBUTION E – Distribution authorized to DoD Components only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office)."
6) DISTRIBUTION F – Further dissemination only as directed by (inserting controlling DoD office) (date of determination) or higher DoD authority." Distribution Statement F may be applied under rare and exceptional circumstances when specific authority exists or when need-to-know must be verified.
7) DISTRIBUTION X – Distribution Statement "X" is superseded by issuance of this Instruction. Subsequent dissemination of formerly Distribution Statement X documents shall display Distribution Statement C, with export control as the reason and shall be marked as directed in paragraph 8.a of Enclosure 3, unless changed by the controlling DoD office.

1.7.2 HANDLING AND DESTROYING LIMITED DISTRIBUTION DOCUMENTS

Limited Distribution documents shall be handled using the same standard as "Controlled Unclassified Information (CUI)" material and will be destroyed by any method that will prevent disclosure of contents or reconstruction of the document. When local circumstances or experience indicates that this destruction method is not sufficiently protective of unclassified limited information, local authorities may prescribe other methods but must give due consideration to the additional expense balanced against the degree of sensitivity.

SAMPLE

1.7.3 EXPORT CONTROL WARNING

All technical documents that are determined to contain export-controlled technical data shall be marked "WARNING – This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App. 2401, et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25."

2. CRITICAL INFORMATION (CI)

The definition of critical information refers to all information, operations, and activities to be undertaken in performance of the contract that might reveal information necessary to the success of the program. OPSEC cannot protect everything, so the most important items should be afforded the greatest protection. The following pieces of critical information are those items of the **(program name)** program that have vulnerabilities identified. Amendments to this OPSEC Plan and CI list will be made as additional CI are identified.

(**Use the CI provided by the Contracting Officer. If you feel others are appropriate, add them, but keep list to 10 items or less. Think about your capabilities, activities, limitations (vulnerabilities), and intentions that if the adversary finds out about them, he could stop or severely hinder your production efforts.)**

1)
2)
3)
4)
5)
6)
7)
8)
9)
10)

3. THREATS

3.1 GENERAL APPLICABILITY

Based upon information provided by JMC and other Government Agencies, the threats applicable to the **(program name)** efforts stem primarily from five sources: Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signatures Intelligence (MASINT) and Open-Source Intelligence (OSINT). The worldwide intelligence collection threat is multi-disciplined, highly sophisticated, and extremely dedicated. Intelligence collection efforts may use only one discipline (or a combination of disciplines) to obtain information. As new threat data is

SAMPLE

received, distribution shall be made to program personnel and other participants in program activities as appropriate.

3.2 HUMAN INTELLIGENCE (HUMINT) THREAT

Human intelligence describes activities to obtain both classified and unclassified information through the use of human agents. Endeavors of human agents (both overt and covert) pose a substantial threat if countermeasures to neutralize or minimize their activities are not employed.

3.2.1 OVERT – OPEN-SOURCE INTELLIGENCE (OSINT) THREAT

Significant quantities of unclassified, highly technical documents (both formal as well as in-house distribution and coordination items) offer a lucrative target to an adversary. Requests for documents relating to the program should be anticipated since many Intelligence Services work through clearinghouses and employ cover organizations in their increasing attempts to collect technology. Literature Intelligence (LITINT) is a category of intelligence information derived from written/printed/graphic and computer database sources. It is information obtained from an analysis of information available to the general public and most often accomplished by overt HUMINT sources. With the development of computers, LITINT has assumed a greater role in worldwide information gathering. Vast amounts of information of significant interest to other governments are available in computerized databases. Computer aided LITINT is a key part of intelligence efforts that are accomplished with minimal risk and cost.

3.2.2 VISITORS

Visitors to the facilities include, but are not limited to government personnel, subcontractors, vendors, suppliers, contract labor organizations and service groups (repairmen, telephone, janitorial, etc.) who may obtain information of interest to an Intelligence Service. The greater danger to the program is the possible visual and aural disclosure of information that could inadvertently occur during these visits.

3.2.3 COVERT – ILLEGAL ENTRY/COERCION/COLLUSION (ESPIONAGE)

While this aspect of HUMINT is normally considered to be the exception rather than the rule, the possibility still exists for these methods to be employed against the program. With joint ventures and international partners, the probability is almost assured. Examples include placing serendipitous listening devices in meeting rooms and foreign aircraft carriers, recruiting agents from the general population and key people who have access to sensitive information, etc. This type of intelligence gathering includes all clandestine and illegal activities and operations of Intelligence Services. Covert operations inflict severe damage and compromise to our country. These items are included as an awareness factor to ensure program participants are fully cognizant of the possible threats from various Intelligence Services.

SAMPLE

3.3 SIGNALS INTELLIGENCE (SIGINT) THREAT

SIGINT describes the capability to obtain classified and certain unclassified information by monitoring communication systems, or by analyzing electromagnetic radiation/emanations from various types of equipment. Most activities and organizations are highly susceptible to the SIGINT threat. SIGINT is derived from signal interception and includes all Communications Intelligence (COMINT), Electronics Intelligence (ELINT) and Foreign Instrumentation Signals Intelligence (FISINT). Telephone conversations are especially vulnerable because most are relayed, at some point in transmission, via microwave signals that are easily monitored. The use of double-talk and self-generated codes is not effective as a means to protect sensitive information during telephone conversations. Professional intelligence analysts easily defeat these procedures.

3.4 IMAGERY INTELLIGENCE (IMINT) THREAT

IMINT describes the capability to derive information from imagery developed over the full range of the electromagnetic spectrum. Intelligence Service representatives see a distinct danger in the employment of clandestine photography. Applications of IMINT include: Hand-held photography; satellites, scheduled commercial aircraft and private aircraft overflights that employ advanced photographic techniques; and unauthorized use of copying/duplicating equipment. IMINT frequently provides very valuable intelligence. Imagery of experiments or tests can be obtained from land, sea, air and space platforms. The most serious threat from IMINT resources at the national level stems from photoreconnaissance satellites.

3.5 MEASUREMENT AND SIGNATURES INTELLIGENCE (MASINT) THREAT

MASINT is technically derived intelligence that detects, locates, tracks, identifies, and describes the unique characteristics of fixed and dynamic target sources. MASINT contributes both unique and complementary information on a wide range of intelligence requirements and is often the basis for cross-cueing other collection disciplines. It is considered highly reliable since it collects performance data and characteristics on actual targets that do not intend to create an indication of presence or activity. MASINT target signatures are converted into threat recognition and identification profiles and the surveillance, tracking, discrimination, and engagement algorithms that guide smart weapons. Civil applications can include timely warning of forest fires and volcanic eruptions, tracking volcanic ash clouds, detecting pollution sources, and providing data on natural phenomena to support environmental studies.

3.6 INTELLIGENCE COLLECTION THREATS TO (**COMPANY**)

The following analysis of threat is from unclassified sources. There is a consensus within the U.S. Intelligence Community that such collection efforts face almost all contractors developing and producing technologies. Any business enterprise operating in the global competitive market should recognize that it is continually targeted by intelligence collection efforts.

SAMPLE

3.6.1 WORLDWIDE GENERAL THREAT

Pervasive worldwide multi-discipline information collection activities are being conducted against U.S. contractors on a daily basis. Increasingly significant resources are devoted to monitoring activities of U.S. Defense contractors. Clearly, our adversaries can produce reliable information on business capabilities, vulnerabilities, and intentions. The intelligence threat to the U.S. economic and scientific base has actually increased dramatically since the end of the cold war.

3.6.2 CHANGING NATURE OF THE WORLDWIDE THREAT

The collapse of the Soviet Union (now the Commonwealth of Independent States – (CIS)) in December 1991 intensified the intelligence collection threat posed by foreign countries. That collapse allowed the redirection of collection efforts from the military to technological and economic interests. Our traditional adversaries continue to conduct intelligence activities. Over 50 Third World governments, using intelligence training received from former Soviet Union bloc countries, continue to act unilaterally in intelligence collection. Nontraditional adversaries, 94 out of 171 countries studied, target the U.S. Over 20 nations (both friends and foes) have been identified as conducting economic espionage activities against U.S. Corporations. They target any information that will give their indigenous companies an edge in the world marketplace. This economic espionage is expected to continuously increase in the near future with the main target being the theft of "core" technologies. To a lesser degree countries in Asia, Europe, the Middle East and Latin America are also collecting. The most active countries are the CIS, Israel, France, and Japan. The most proficient are China, Japan, France, Israel, Sweden, Switzerland and Britain. Foreign Countries use this type of intelligence to directly support business - - their spying easily pays for itself. They target not only western technology to help their country's industry compete in the world marketplace, but also seek to obtain financial and commercial information to gain an immediate bottom-line advantage in the world marketplace.

3.6.3 INTELLIGENCE COLLECTION THREAT TO **(COMPANY NAME)**

The threat to operations of the U.S. or individual companies arises from the capabilities of hostile countries, friendly countries, or competitors, to piece together bits of information. Information is analyzed over time to determine patterns and to assign meanings to detectable activities. Generally, competitive analyses and estimates are very valuable if they are 70% correct. At 100% correct, these predictions are invaluable to our competitors or adversaries.

(**Fill in the threat information provided by the Contracting Officer.)**

SAMPLE

4. VULNERABILITIES

Vulnerabilities of the program may reveal sensitive or classified information, operations, plans and/or activities, and are derived by comparing the threat to the sensitive aspects of the contract and assessing the OPSEC Indicators.

4.1 GENERAL VULNERABILITIES

The following vulnerabilities are most commonly identified in an OPSEC assessment.

1) Lack of OPSEC Awareness - Personnel do not fully realize their OPSEC responsibilities. Employees are not aware of the extent to which an adversary depends on obtaining unclassified information on a defense project and their capability to decipher important intelligence data from this seemingly non-critical information.

2) Testing - subsystem testing may be vulnerable to exploitation.

3) Open-Source Literature - Even unclassified information released to the news media, or at meetings, seminars, and through contractor advertisements, may provide analytical centers with valuable information regarding individual systems capabilities, limitations and technical operations.

4) Professional Conferences/Symposia - Program personnel are susceptible to elicitation and exploitation when attending these events by fellow participants who covertly represent the intelligence collection agencies of foreign governments. Collection efforts may range from innocuous questions from foreign scientists to actual blackmail by intelligence agents. Without constant awareness of the threat, project personnel may inadvertently release information of analytic value.

5) Communications - All unsecured telephone conversations (including cellular phones) are vulnerable to monitoring, and all long-distance microwave transmissions are subject to intercept. Such vulnerabilities provide a source of information for intelligence agents. Communications supporting computer systems and faxes are equally vulnerable.

6) Subcontracting - The prime contractor may fail to recognize the need for the imposition of OPSEC on its subcontractors.

7) Automated Information Systems (AIS) Operations - Without adequate security measures, AIS are susceptible to intrusion or tampering through both hardware and software manipulation. Further, the emanations from AIS equipment and power lines may be subject to intercept.

8) Visitor Control - Visitors within the facility may observe or hear sensitive information, operations, or activities.

9) Conference Room Security - Classified and sensitive information could be compromised by covert listening devices installed in meeting rooms frequently used for sensitive discussions.

10) Disgruntled Employees and Employees with Personal Problems (Adverse Information) - Personnel possessing security clearances who, through personal adversities or circumstances such as marital difficulties, criminal behavior, excessive indebtedness, and/or indiscriminate use of alcohol, present attractive targets to Intelligence Services. Supervisors and/or fellow employees may become aware of these difficulties but may fail to notify management or security to investigate, electing to ignore the problem or

SAMPLE

rationalizing that some other party will take action. Non-action on the part of personnel who become aware of these situations can be as significant as that presented by an adversary who may attempt to exploit personnel experiencing these problems.

4.2 CONTRACTUAL VULNERABILITIES

In addition to the vulnerabilities identified above, these vulnerabilities are specific to (**program name**). **(INSERT VULNERABILITIES IDENTIFIED FOR THIS PROGRAM. CONSIDER THESE POSSIBLE SOURCES OF VULNERABILITY)**

1) Use of a commercial travel office, travel patterns, and travel practices.
2) Geographic separation of the program participants.
3) Limitations of export license(s).
4) Effectiveness of the product.
5) Sympathies of program personnel for adversary countries.
6) Outdoor testing which results in exposure of the program to overhead (imagery) threats, HUMINT observation, etc.
7) Communications between test sites and program offices following testing.
8) Lack of procedures or failure to comply with those developed for controlling visits and documents/information release to international partners and subcontractors.
9) Unauthorized access to specific unclassified performance parameters related or identified with the program.

5. ASSESSMENT OF RISK

The purpose of this step is to select which of the tentative OPSEC measures to implement based on the threat and vulnerabilities identified. The Contractor must balance the risk of operational failure against the cost of OPSEC measures. Consider the following questions for each tentative measure.

1) What is the likely impact of an OPSEC measure on operational effectiveness if implemented?
2) What is the probable risk to mission success if the Company does not implement an OPSEC measure?
3) What is the probable risk to mission success if an OPSEC measure does not work?
4) What is the impact on future missions if this measure is adopted and successful?

6. OPSEC MEASURES

Analysis of vulnerabilities identifies OPSEC measures required to protect sensitive information under the **(company name)**'s control. The most desirable OPSEC measure combines the highest protection with the least impact on the (**program name**) effectiveness.

6.1 GENERAL OPSEC MEASURES

SAMPLE

1) Education - (**Company name**) will use education and training to eliminate vulnerabilities discovered through ongoing OPSEC analysis. Participants (including new hires, consultants, transferees, contract labor personnel and subcontractors) shall be briefed and kept informed (through bulletins and/or revised OPSEC guidance) of all sensitive aspects of the Program and the measures designed for the protection of this information and the need for continued awareness and enforcement of OPSEC principles. Program participants will be briefed concerning the OPSEC significance of their day-to-day tasks, as the activities and operations undertaken in performance of the contract may communicate sensitive information to unauthorized persons just as well as documents produced.

2) Open-Source Literature - Procedures are established within (company name) to ensure no public release concerning program information occurs without the prior written approval of the JMC. OPSEC consideration shall be included in the review cycle. Reviews shall also be conducted on announcements concerning visits, tests, and activities posted within facilities about Program matters. Subcontractors are required to forward all material for public release through (company name) for approval prior to releasing the material.

3) Communications - Emphasis will be placed on instilling awareness among program participants concerning the use of communication devices. Aspects of Communications Security (e.g., e-mails, data fax & cellular phones) will be included in the awareness briefings.

4) Subcontractor Flow-down of OPSEC - All subcontractors' Statement of Work will be reviewed by the OPSEC Coordinator prior to award of contractual work to determine OPSEC applicability.

5) Visitor Control - All visitors are required to process through established checkpoints for verification of identity, citizenship, personnel security clearances, appropriate certification of purpose of visit, issuance of badges, inspection of articles being brought into and out of the facilities and other such measures to assure proper visitor control. Escort for visitors shall be advised of proper escort procedures, limitation on disclosure, and other applicable controls involved in the visit. Program personnel shall be reminded through OPSEC briefings of the potential for the inadvertent release of information by visual and aural means when visitors are present. Activities of visitors and non-assigned personnel in the program areas shall be observed to determine that their presence is required by business needs and that no suspicious activities are detected which may pose a threat to the security of information.

6) Conference Rooms - Program participants will be reminded of conference room procedures to be employed when discussing classified and sensitive unclassified program matters. This will include attendance control, procedural security while the conference is in session, instruction on note taking, disclosure of the classification/sensitivity of information being discussed, and procedures to ensure that all material is protected during the session, during breaks, and from removal when the session ends.

6.2 CONTRACTUAL OPSEC MEASURES

SAMPLE

(LIST ANY ADDITIONAL COUNTERMEASURES REQUIRED that you have identified and are implementing FOR YOUR PROGRAM)

7. SELF-ASSESSMENT OF OPSEC PROGRAM

The (**Company name**) OPSEC Coordinator conducts annual self-assessments of the (Company name)' s OPSEC Program to determine the viability of the program via a formal OPSEC checklist that has been developed tailored to the Company's needs. As a minimum, the following are assessed:

1) Identification of critical information
2) Employee's knowledge of critical information
3) Employee's knowledge of the collection threat to the company
4) OPSEC measures in place to protect critical information
5) The status of the company's training.

The OPSEC Coordinator submits an annual written assessment with results and recommendations to the Contracting Officer who will forward to the JMC OPSEC Office for review and retention.

8. TRAINING AND AWARENESS

8.1 GENERAL

For the OPSEC program to be effective, Facility personnel must understand the concept and importance of OPSEC and apply that knowledge and awareness in the performance of their everyday tasks. Successful OPSEC training and awareness will be gauged by individuals being able to answer three primary OPSEC questions:

a. Why is OPSEC important to my Facility/organization/department?
b. Why is OPSEC important to me?
c. How can I contribute to OPSEC? Employees must know who their Facility OPSEC officials are, and how to contact them for questions or concerns on OPSEC related issues.

8.2 INITIAL OPSEC TRAINING/ORIENTATION

OPSEC orientation training will be provided as part of the in-processing of newly assigned personnel within 30 days of arrival. Training will be provided by the Installation/facility OPSEC Officer or OPSEC Coordinator. Focus of the training should include an overview of the intelligence threat to all personnel, the collection methods an adversary will use to collect information and the appropriate OPSEC measures to be taken to protect specific sensitive information pertinent to the individual's job.

8.3 REFRESHER OPSEC TRAINING

Facility personnel will receive refresher training annually either in person or through an approved DOD on-line training package.

8.4. OPSEC AWARENESS

SAMPLE

At least once quarterly, promote OPSEC awareness by publishing OPSEC bulletins, displaying OPSEC posters, disseminating OPSEC information or reminders via electronic communications (e-mail, marquees, etc.), or conducting in-person interviews with personnel. Coordinators and supervisors should make on-the-spot corrections of poor OPSEC practices and continuously use good OPSEC practices which will stress the important of OPSEC to mission success.

8.5. TRAINING OF DESIGNATED OPSEC OFFICIALS
The OPSEC Coordinator will complete OPSEC Level II certification training by attending the Headquarters Department of the Army (HQDA) OPSEC Officers Course or a Service equivalent Operations Security Program (NOP) course. Additionally, it is recommended the OPSEC Coordinator receive external official presence (EOP) training.

8.6. OPSEC TRAINING RESOURCES
•Center of Development of Security Excellence (CDSE), OPSEC Awareness for Military Members, DOD Employees and Contractors:
https://securityawareness.usalearning.gov/opsec/index.htm
•OPSEC Professionals Society; http://www.opsecsociety.org/
•Operations Security Professional's Association (OSPA);
http://www.opsecprofessionals.org
•Naval OPSEC Support Team (NOST), Navy Information Operations Command (NIOC);
http://www.public.navy.mil/fcc-c10f/niocnorfolk/Pages/OPSECMission.aspx
•Center for Development of Security Excellence (CDSE), Defense Security Service (DSS);
http://www.cdse.edu/index.html
•National Counterintelligence and Security Center (NCSC) Enterprise Threat-Mitigation Directorate (ETD) and the National Operations Security Program (NOP);
https://www.dni.gov/index.php/ncsc-what-we-do/operations-security

8.7. CUI
For the CUI program to be effective, facility personnel must understand the concept and importance of CUI and apply that knowledge and awareness in the performance of their everyday tasks.

8.8. CUI AWARENESS
Coordinators and supervisors should make on-the-spot corrections of poor CUI practices and continuously use good CUI practices which will stress the important of CUI to mission success.

8.9. CUI TRAINING RESOURCES
•DoD CUI Program; https://www.dodcui.mil/
•Center for Development of Security Excellence, Defense Counterintelligence and Security Agency, DoD Mandatory Controlled Unclassified Information (CUI) Training:
https://securityawareness.usalearing.gov/cui/index.html

SAMPLE

ACRONYMS

AIS	Automated Information Systems
CI	Critical Information
CIS	Commonwealth of Independent States
COMINT	Communications Intelligence
CUI	Controlled Unclassified Information
DoD	Department of Defense
ELINT	Electronic Intelligence
FISINT	Foreign Instrumentation Signals Intelligence
FOIA	Freedom of Information Act
HUMINT	Human Intelligence
IMINT	Imagery Intelligence
JMC	Joint Munitions Command
LITINT	Literature Intelligence
MASINT	Measurement and Signatures Intelligence
OPSEC	Operations Security
OSINT	Open-Source Intelligence
SIGINT	Signals Intelligence
U.S.	United States

REFERENCES

AR 530-1	Operations Security	26 September 2014
DoDI 5200.01	DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI),21 April 2016, Incorporating Change 2, 1 October 2020	
DoDI 5230.24	Distribution Statements on Technical Documents	10 January 2023
DoDD 5230.25	Withholding of Unclassified Technical Data from Public Disclosure 6 November 1984 Incorporating change 2, 15 October 2018.	
DoDI 5200.48	Controlled Unclassified Information (CUI)	6 March 2020

SAMPLE