INTEGRATING OPSEC INTO CONTRACTS

A Companion Guide to the OPSEC Practitioner's Toolbox

February 2008

TABLE OF CONTENTS

I. OPSEC In Contracts

A. Protecting Your Critical Information

The Interagency OPSEC Support Staff (IOSS) developed this guide to help you, the operations security (OPSEC) practitioner, expand the protection of your critical information into your contracting process, before and after contract award. This is a primer, teaching general principles, and does not focus on a particular Federal department or military service. This guide is intended to help you work with your organizational leaders, program managers, technical and administrative staff, industrial security and contracting personnel as you facilitate the development of contractual OPSEC requirements for specific programs and their contracts. We emphasize the use of this guide for development contracts or contracts where work is being performed off-site and contractors are not integrated into the Government workforce or OPSEC training programs. While we have included sample OPSEC plans, it is **not** intended that you use it separately from the principles expressed in the *Practitioner's Toolbox.*

This guide is based on the experience gained by the IOSS from a pilot project, from OPSEC and contracting experts throughout the Government and contracting community, and from our students and conference attendees. We welcome your feedback because it helps us to continually improve our products and services.

B. Mitigating Risks

Risk is a result of probabilities and consequences. Through the principles of OPSEC, we explain this in terms of threats, vulnerabilities, and the impact if critical information or indicators are noticed, known, or exploited. Impacts may affect your mission, facilities, and personnel.

1. Threats to Your Contractors and Your Critical information

We realize that you probably know why it is important to include OPSEC in contracts. However, we know how difficult it can be to gain endorsement for your Government OPSEC program, where costs are often indirect. We realize how much harder it can be to convince your leaders to allocate money for contractual OPSEC requirements. We recommend that you invest the time in investigating and analyzing threats that are specific to your organization, program, and contractors. The more specific your threat information, the more powerful your message will be to your leaders. We include some information that may help you frame that threat data.

In general, when your unclassified information is being created, stored, processed or transmitted by a contractor it is exposed to threats that are similar to those you are already trying to protect against:

- Foreign Intelligence;
- Terrorists;
- Criminals;

- Business Competitors;
- Disgruntled Employees;
- Dishonest Employees; and,
- Hackers.

Foreign intelligence services pose great threats because they often fund and direct the activities of foreign businesses that collect information on their competitors—very possibly your critical information from your contractors. While your critical information is targeted and sometimes easily available to these companies/countries, it is hard to assess what and how much of your information is being exposed and exploited. The Defense Security Service (DSS) publishes an annual report, *Technology Trends in the U.S. Defense Industry*, which presents an assessment based on suspicious contact reports originating from the cleared defense industry. This is a snapshot based on suspicious activity that is detected and reported, and while it does not represent an accurate picture of the threat to critical information, it does show that a wide range of critical information is being targeted by many countries, using a variety of techniques, most of which can be countered by incorporating OPSEC into contracts.

Furthermore, the practices of the competitive intelligence profession and the global investment in such training indicate that foreign corporations are practicing passive and active information collection techniques that are lucrative, even when only legal methods are used and non-proprietary or unclassified information is the target. Their collection practices alone make a strong case for OPSEC in industry and in Government contracts.

2. Vulnerabilities Introduced Through Contracting

The National Industrial Security Program Operating Manual (NISPOM) requires a cleared contractor to protect classified information and to perform certain security functions as overhead without charging the Government. It does not require companies to apply OPSEC or to protect *unclassified* critical information using OPSEC.

When OPSEC requirements are included in Government contracts, often they are written with minimal specificity. To win a contract or contract renewal, companies must make internal choices in how they cost the contracted activity. They must be competitive with other bidders. When non-specific OPSEC requirements imply something, but don't require specific effort, nearly any action will suffice. Actual OPSEC may never be performed within supporting industry activities.

Unclassified critical information determined important to the supported Government activity can be vulnerable to inadvertent loss when it passes through related contractor processes. If the Government sponsor does not create a contractual relationship that allows communication of designated critical information and corresponding requirements for its protection, along with related critical information determined within contracted activity, then Government critical information and missions may be exposed to increased risk.

3. Impact of Exposing Critical information

It is in the best interest of the United States politically, economically and militarily for OPSEC programs to be required for contracts when critical information is identified so that appropriate protective measures are adopted. With the increase in Government outsourcing of sensitive activities and the growth of information collection threats in the marketplace, contractors who are part of the Defense Industrial Base and in particular those whose products are on the Militarily Critical Technologies List (MCTL) need to consider OPSEC. The FBI asserts that billions of dollars are lost to the U.S. economy each year due to foreign economic espionage. The counterintelligence community is well aware of the role that foreign companies play in the intelligence collection activities of nation states.

While the NISPOM requires that classified information be protected, there is a great volume of unclassified information that remains unprotected and available to an adversary. Of grave concern to the IOSS is that this information, especially in aggregate, may be easily exploited by America's adversaries.

4. Need for Specific OPSEC Requirements in Contracts

If a Government sponsor desires specific OPSEC efforts to be performed, specific requirements must be included in contract documentation to establish what the Government wants and is willing to pay for. Competing bidders can now estimate costs for the work and the approved contract establishes an agreement regarding actions to be performed. Compliance reviews are also enabled.

Specific OPSEC requirements cannot be written by personnel who do not understand the organization's OPSEC program and applications. OPSEC practitioners must provide contracting officer representatives with training and options to select from to ensure appropriately specific OPSEC requirements are included in the contract documents. If the sponsoring program and OPSEC practitioners believe the contractor operation needs to be informed of Government-identified critical information requiring protection, the Government OPSEC program should consider including provisions to communicate this information to the contractor with protection requirements.

C. Cost-Effective Contractual Requirements

The way to mitigate the risk to your critical information is to implement contractual OPSEC requirements. We recommend you describe these requirements in a contract OPSEC plan, which you include as an attachment to the statement of work (SOW) in the request for proposal (RFP) and final contract. (A sample is included in this guide which will be discussed in more detail in Section x.) Since contractual OPSEC requirements may incur some level of expense, and because your organization or program does not likely have "extra" funds, this guide proposes ways to introduce OPSEC requirements that can be satisfied within a limited budget. The result will be the cost-effective provision of OPSEC awareness training, which will motivate contract employees to follow the OPSEC Standard Operating Procedures (SOP/countermeasures) to protect critical information.

II. How to Get Started

A. The Government Program's OPSEC Plan

If the Government program that is sponsoring the contract already has its own OPSEC program and critical information list, then you may be ready to facilitate development of the contract OPSEC plan. If the sponsoring Government program already has an OPSEC plan and program in place, it will be easier for you to update the threat and vulnerability data that will be part of the OPSEC awareness training, and you may have a much better idea of the cost-effective countermeasures to require.

Where no plan exists, you may use the information provided in the *OPSEC Practitioner's Toolbox* or appropriate organizational guidance to develop your OPSEC program and any OPSEC plans deemed necessary. You will serve as the facilitator and work with organizational leaders, the program manager, the technical and administrative staff, and contracting personnel. The goal is to ensure that critical information is identified and protected through implementation of an OPSEC plan that protects the Government program and that this same information is protected on any contracts.

You will facilitate the development of a list of critical information that this OPSEC program needs to protect; the more specific the list, the more effective your program will be. You will lead: the research and analysis of specific threats to the program; identification of key vulnerabilities, impact, risk assessment; and, development of countermeasures. Use the information provided in the *Practitioner's Toolbox* to implement the five-step OPSEC process and to develop the OPSEC plan and OPSEC data for this program. For the purposes of this paper, we consider the resulting OPSEC data to be:

- Critical information;
- Threat assessment;
- Vulnerabilities; and,
- Countermeasures.

The sponsoring Government program's OPSEC data will be used to develop: the contract OPSEC plans, associated OPSEC data, and annexes to the contract OPSEC plan. Impact and risk are not included separately on this OPSEC data list because they are part of the analysis that derives the list of countermeasures, or the standard operating procedures (SOP) for the contract.

B. The Contract OPSEC Plan

Once the Government program has its own OPSEC plan and critical information list, you can more easily facilitate the development and updates of the critical information list and other OPSEC data for the contract OPSEC plan. In the case of the contract, it is critical to involve the right people to ensure that the right countermeasures, training methods and populations are included in the contract OPSEC plan, and that the decision makers, including the program manager, are involved in making determinations about the critical information list, training methods, countermeasures, and the number, type and location of personnel who will be part of the OPSEC program. The SOP is the document that includes the list of countermeasures you have directed the contractor to follow, and should be provided with the critical information that you want the contractor to protect. Even if all contractors voluntarily decide to have corporate OPSEC programs that can be expanded to protect Government-specified critical information, the contract OPSEC plan is a primary vehicle for: (1) identifying to the contractor what the critical information is; and, (2) influencing the practice of Government-specified countermeasures.

Technical and administrative program personnel can be particularly useful in determining OPSEC data and helping to cost out the training and countermeasure expenses. Contracting personnel will eventually review the SOW and its attachments, including the OPSEC plan, and can be of great assistance if involved from the beginning as you draft your SOW paragraph and OPSEC plan.

C. IOSS Recommendations

1. Government Provides the OPSEC Requirements/Plan

We recommend that you, the Government OPSEC practitioner, ensure that the OPSEC plan is provided to the contractor. Whenever possible, we recommend against the OPSEC plan being a deliverable on a Contract Data Requirements List (CDRL) or Data Item Description (DID). By your developing the OPSEC plan and its annexes, the Government will save time and money, and retain control over the OPSEC plan and price.

In cases where the Government relies heavily on industry experts and you do not have enough information to develop the critical information list, then you will need to use threat data and dialogue with the contractor about threat and impact to derive a critical information list, which the Government must approve. This will often be the method in cases where the contracted work is specialized or technical; the critical information may closely resemble Critical Program Information (CPI) that is required for programs that have mandatory Program Protection Plans. Critical information is often a subset of CPI. Even when the contractor must play a significant role in drafting the critical information, we recommend that you use the contract OPSEC plan template included in this guide to save time and money.

2. Apply OPSEC to Contracting Processes

As the OPSEC practitioner, you can ensure that OPSEC is applied before the contract is awarded by conducting an overall review of the program’s Invitation for Bid, RFP, and Request for Quote.

a. Influence documentation to restrict the unnecessary release of critical information, while still allowing potential bidders to estimate costs. Regarding the OPSEC plan, necessary data includes:

- Hours for OPSEC Program Personnel to work on OPSEC Program (training, program management);

- Hours for contract employee OPSEC awareness training;
- Hours for Personnel to Participate in OPSEC Program;
- Travel costs; and,
- Cost of materials and equipment.

b. As part of good OPSEC practices before contract award, include only general information in the “shell” OPSEC plan and provide more detail in the following contract OPSEC plan annexes separately, after contract award, since they are sensitive and only the award winner has a need-to-know. If one or all annexes need contractor involvement to develop, then they should be discussed after contract award.

Annex A: Critical information
Annex B: Threat (often classified)
Annex C: Vulnerabilities (often classified)
Annex D: SOP/Countermeasures

Impact and risk are omitted because they are part of the analysis that derives the SOP/countermeasures for the contract.

c. Influence communication practices used during solicitation stage (e.g., have contractors send in proposals via mail and secure fax instead of non-secure fax and the Internet and use secure voice instead of non-secure voice as appropriate).

d. Prepare Government personnel before any pre-bid conference.

As the OPSEC practitioner, you can influence required contractor practices after the contract is closed, to include:

a. Directing contractors to destroy records using specified methods after contract execution.

b. Restricting contractors from advertising their work on this contract without consent from the Government and the OPSEC program. (See DD Form 254, item 12.)

3. Government Provides OPSEC Training

We recommend that regular, mandatory OPSEC awareness training be delivered in a web-based format with necessary updates to the critical information list and SOP/countermeasures provided via e-mail or hardcopy. (The costs to provide two to four hours of classroom training per year may be beyond OPSEC budget allocations for many programs.)

The IOSS recommends the use of “An Introduction to OPSEC: An Interactive Primer by the Department of Defense,” which includes general awareness of OPSEC, some threats, and vulnerabilities. This computer-based training, which includes built-in quizzes, may be centrally loaded on a company’s intranet, made accessible to all employees, and tracked for accountability. You will need to augment this with more specific threat and vulnerability information to motivate your contract employees.

III. Developing the Contractual Documentation

A. Paragraph for Statement of Work (SOW)

We recommend that the OPSEC requirements, even if minimal, be provided in a “detachable” OPSEC plan, which is an appendix to the SOW. This way, the OPSEC requirements are not buried in contract language and can be provided separately to the OPSEC points of contact at the company. Here is a sample OPSEC requirements paragraph to be included in your SOW.

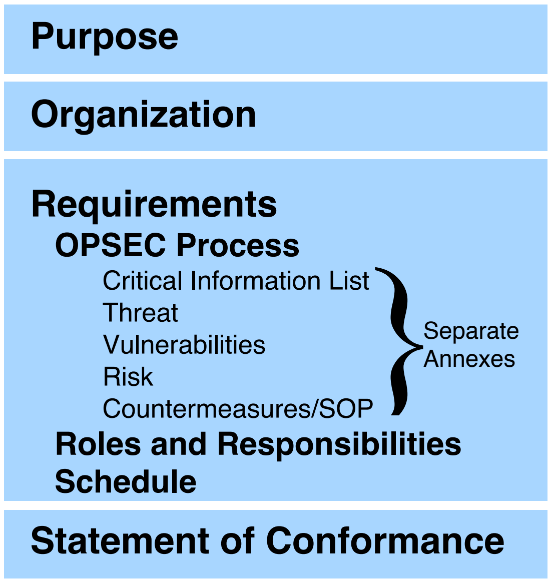
> All contractors (including subcontractors) identified in the Operations Security (OPSEC) Plan under appendix C of the Statement of Work shall supplement their current security practices by requiring any personnel involved in executing the XYZ contract to complete Government-sponsored and administered Operations Security (OPSEC) training. Upon contract award, all identified contractors (including subcontractors) shall sign the contractor's conformance statement contained within the Operations Security (OPSEC) Plan and submit it to the [Government agency] contracting officer thereby acknowledging that they will meet the requirements of the XYZ PMO generated OPSEC Plan. The contractor specialist security officer (CSSO) shall contact the contracting officer or designated contracting officer's representative (COR) in accordance with the OPSEC Plan to schedule key employees to attend the Government-sponsored OPSEC training. The contractor must immediately notify the Government upon the discovery of any non-conformance with the OPSEC Plan.

B. Appendix to SOW: Contract OPSEC Plan

The way to mitigate the risk to your critical information is to implement contract OPSEC requirements. We recommend you describe these requirements in a general or “shell” contractual OPSEC plan, which you include as an attachment to the SOW in the RFP and final contract. We recommend an OPSEC Plan as it will contain all necessary administrative information that could be omitted if you merely include an OPSEC paragraph in the SOW or, worse, if you only include a brief statement on the DD Form 254.

It is recommended that the Government develop and provide a contract OPSEC plan as an appendix to the SOW, instead of making the OPSEC plan a deliverable. This way, the Government sponsor saves time and money on a contract and exerts and retains control over the OPSEC plan and saves the contract costs of OPSEC plan development. It is recommended that the Government sponsor provide a “shell” OPSEC Plan during the solicitation stage as part of the RFP/SOW. Below we have included the framework for a sample contract OPSEC Plan, which does not include annexes. By providing this “shell” OPSEC plan, all potential bidders can view the contract OPSEC plan, but only the winning company receives the contract’s critical information list, threat analysis, SOP/countermeasures and training materials.

1. Structure of "Shell" Contract OPSEC Plan



Purpose

Organization

Requirements

OPSEC Process

Critical Information List
Threat
Vulnerabilities
Risk
Countermeasures/SOP

Separate Annexes

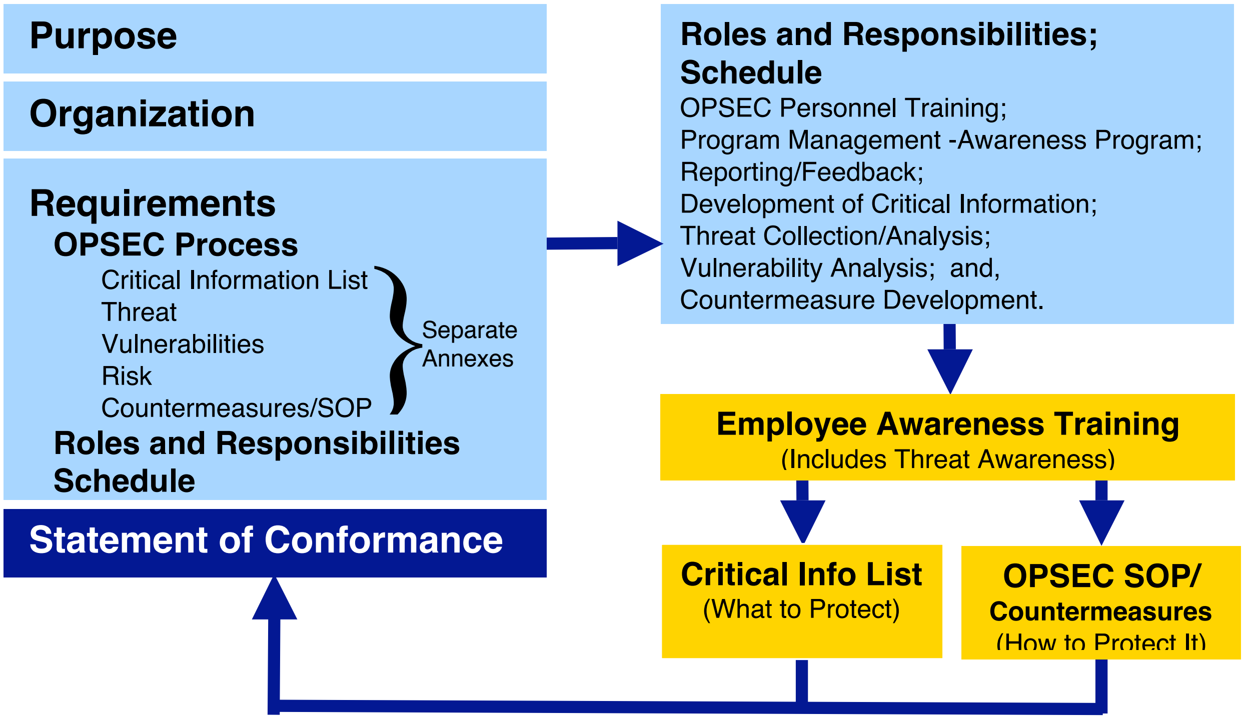
Roles and Responsibilities

Schedule

Statement of Conformance

2. Work Flow of Contract OPSEC Plan with Annexes

The OPSEC process is facilitated through the contract, and the roles and responsibilities of the government organization's OPSEC practitioner, the OPSEC officers at the prime contractor (or Lead System Integrator (LSI)), as well as the OPSEC coordinators at each subcontractor.



Purpose

Organization

Requirements

OPSEC Process

Critical Information List
Threat
Vulnerabilities
Risk
Countermeasures/SOP

Separate Annexes

Roles and Responsibilities

Schedule

Statement of Conformance

Roles and Responsibilities; Schedule

OPSEC Personnel Training;
Program Management -Awareness Program;
Reporting/Feedback;
Development of Critical Information;
Threat Collection/Analysis;
Vulnerability Analysis; and,
Countermeasure Development.

Employee Awareness Training
(Includes Threat Awareness)

Critical Info List
(What to Protect)

OPSEC SOP/ Countermeasures
(How to Protect It)

🟦 **OPSEC Program Personnel Activities**

🟨 **Contractor Workforce Activities**

C. A Sample “Shell” Contract OPSEC Plan

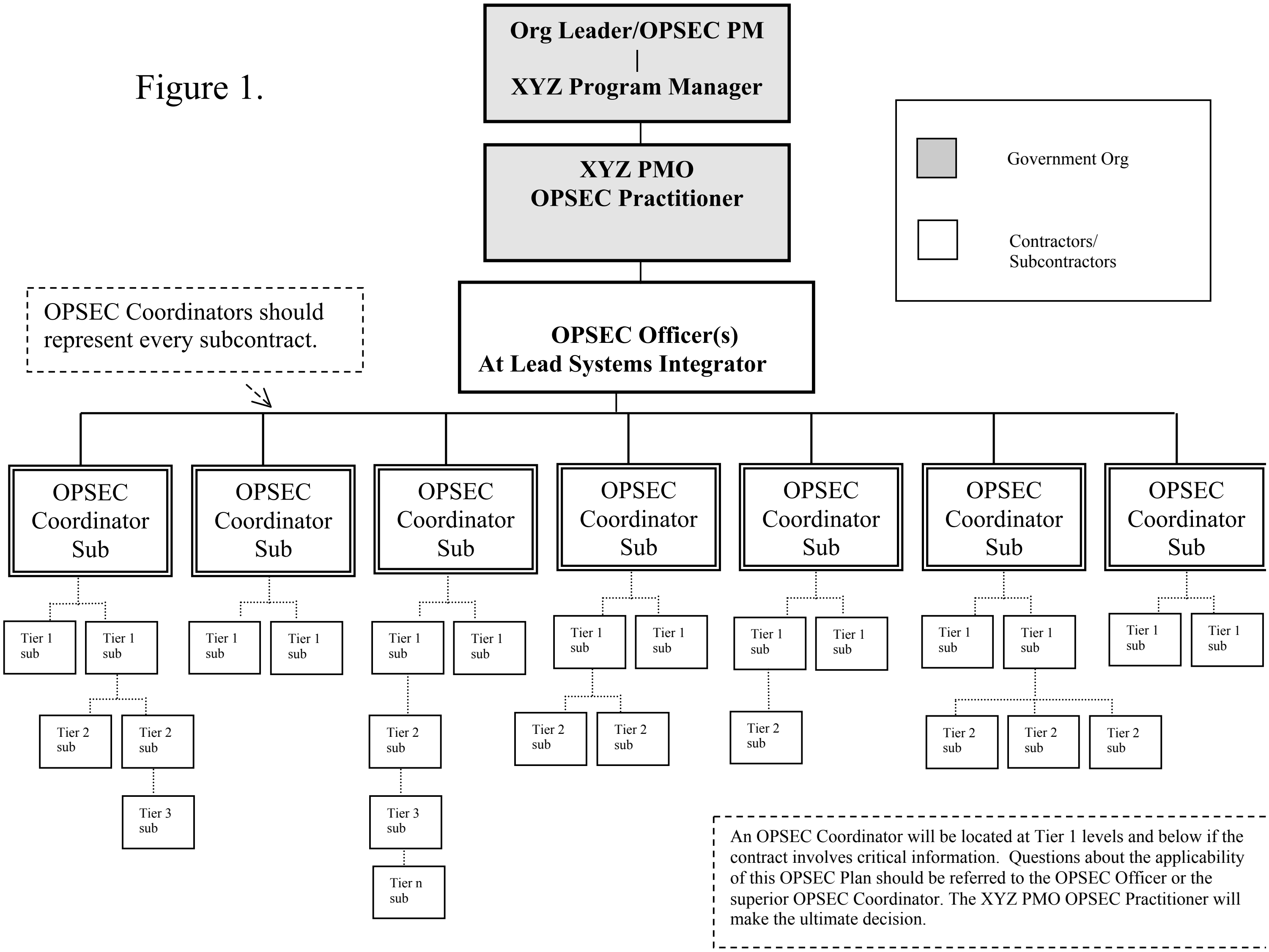
The XYZ Program Operations Security (OPSEC) Plan is included here for your information with clarifying notes in the blue boxes.

XYZ Program
OPERATIONS SECURITY (OPSEC) PLAN
5 June 2007

1. PURPOSE: The OPSEC Program will provide the structure to ensure that OPSEC requirements are met for the XYZ PMO programs and activities involving the Lead Systems Integration (LSI) contract as well as all subcontracts involved with the development of the XYZ. This plan is based upon the results of XYZ PMO's OPSEC process and is intended to protect critical information related to the XYZ development, as well as information about the XYZ PMO, its contracts, and subcontracts. While critical information, indicators, threat information, risk assessment, OPSEC Standard Operating Procedures (SOP), and all updates will be provided under separate cover, this plan covers general vulnerabilities and the required countermeasures that will mitigate and lower risk to the XYZ development.

2. ORGANIZATION: This OPSEC Program and its requirements apply to all contracted and subcontracted elements and personnel supporting the XYZ PMO. Personnel will participate in the OPSEC program under the following management structure (see Figure 1):

Figure 1.



OPSEC Coordinators should represent every subcontract.

An OPSEC Coordinator will be located at Tier 1 levels and below if the contract involves critical information. Questions about the applicability of this OPSEC Plan should be referred to the OPSEC Officer or the superior OPSEC Coordinator. The XYZ PMO OPSEC Practitioner will make the ultimate decision.

2.1. This OPSEC Program shall have an OPSEC Officer, employed by the Lead System Integrator (LSI), who will be assigned to this duty up to 10%, on average, throughout the duration of this contract. The OPSEC Officer is the XYZ PMO OPSEC Practitioner's main point of contact for all OPSEC issues related to this contract. The XYZ PMO OPSEC Practitioner may require that the LSI identify a team of OPSEC Officers each to be assigned to OPSEC duties up to 10%, on average, throughout the course of this contract.

Based on man-hours, 10% was chosen as the affordable amount of time needed to execute the contract OPSEC plan adequately.

Depending on the funding available, it may be more effective to have a team of OPSEC officers from the LSI run the OPSEC programs for subcontracts.

2.2. There is an OPSEC Coordinator on each subcontract, assigned to this duty up to 10%, on average, throughout the course of this contract.

Based on man-hours, 10% was chosen as the affordable amount of time needed to execute the contract OPSEC plan adequately.

2.3. All OPSEC-related communication between the XYZ PMO OPSEC Practitioner and OPSEC Coordinators at subcontractors must be facilitated by the OPSEC Officer(s) at the LSI.

Legal restriction.

3. REQUIREMENTS:

3.1. OPSEC Process.

3.1.1. Critical information. An critical information list and updates will be provided under separate cover after contract award (Annex A) to the OPSEC Officer(s) at the LSI for dissemination to contracted and subcontracted employees who are supporting the XYZ contract, involved in XYZ technical development, and handling critical information. For cost estimating purposes, consider that the OPSEC Plan will apply to all contracts and subcontracts involved in technical development and that 75% of all personnel will handle this critical information.

Critical information will be provided separately to the winners of the contract and to subcontractors which are part of the OPSEC program.

This wording is intended to restrict the cost of the OPSEC program to the appropriate employees.

3.1.2. Threat Assessment. Capable adversaries collecting unclassified, as well as classified, information on the XYZ and similar technologies may pose a threat to the XYZ program, its contractors, and its subcontractors. A formal threat assessment and all updates will be provided under separate cover after contract award (Annex B) to the OPSEC Officer(s) for dissemination to contracted LSI employees and to OPSEC Coordinators at subcontractors for further dissemination to subcontractors who are support the XYZ contract, are involved in technical development, and handle critical information. A general threat assessment is provided below.

Threat information will be provided separately to the winners of the contract and to subcontractors which are part of the OPSEC program.

3.1.2.1. General Threat Assessment. The worldwide intelligence collection threat is comprised of multi-disciplined, highly sophisticated, and extremely dedicated adversaries. There is a consensus within the U.S. Intelligence Community that their collection efforts target almost all DoD contractors developing new technologies. Any business enterprise operating in the global competitive market should recognize that it is continually targeted by intelligence collection efforts. Adversaries can produce reliable information on business capabilities, vulnerabilities, and intentions. Moreover, the intelligence threat to the U.S. economic and scientific base has increased dramatically in recent years.

A list of specific vulnerabilities will be provided separately to the winners of the contract and to subcontractors which are part of the OPSEC program.

3.1.3. Vulnerability Analysis. Vulnerabilities (and indicators) of the program may reveal critical information. A general and contractual vulnerability analysis is provided below. A more detailed list will be provided after contract award (Annex C) to OPSEC Officer(s) for dissemination to contracted and subcontracted personnel who support the XYZ program, are involved in technical development, and handle critical information.

3.1.3.1. General Vulnerability Analysis. The following general vulnerabilities are most commonly identified in an OPSEC assessment.

- Lack of OPSEC Awareness. *Personnel do not fully realize their OPSEC responsibilities. Employees are not aware of the extent to which adversaries depend on obtaining unclassified information on a defense project and their capabilities to derive important intelligence data from seemingly non-critical information.*

- Testing. *Subsystem testing may be vulnerable to exploitation.*

- Open Source Information. *Unclassified information released to the news media (i.e., through meetings, seminars, conferences and exhibitions, contractor advertisements and other public releases, company websites, blogs, emails, professional journals, research papers, conference presentations, resumes, newsletters, annual reports, etc.) may provide adversaries with valuable information regarding individual systems capabilities, limitations and technical operations.*

- Trash. *Much of the open source information described above will be discarded in accessible trash receptacles if it is not protected.*

- 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 blackmail by intelligence agents. Without constant awareness of the threat, project personnel may inadvertently release information of analytic value.*

- Communications. *All unsecured telephone conversations, including faxes, cell phones and Voice over IP conversations, are vulnerable to monitoring. Email and attachments are also vulnerable to interception and monitoring. Such* *vulnerabilities provide a source of information for intelligence agents and other adversaries.*

- Subcontracting. *Contractors at all levels may fail to recognize the need for the imposition of OPSEC requirements in subcontracts.*

- Visitor Control. *Visitors within the facility may observe or overhear critical information regarding operations, activities, etc.*

- Conference Room Security. *Critical information can be compromised if there are no procedures in place to control discussions. Critical information can be compromised by covert listening devices installed in meeting rooms frequently used for discussions.*

3.1.3.2. Contract Vulnerability Analysis. The following contract vulnerabilities are most commonly identified in an OPSEC assessment:

- *Use of a commercial travel office, travel patterns, and travel practices;*
- *Geographic separation of the program participants;*
- *Sympathies of program personnel for adversary countries;*
- *Communications between test sites and program offices following testing;*
- *Lack of procedures or failure to comply with those developed for controlling visits;*
- *Lack of procedures or failure to comply with procedures regarding information release to media, international partners, and subcontractors; and,*
- *Unauthorized access to specific unclassified performance parameters related or identified with the program.*

3.1.4. Risk Assessment. The XYZ PMO OPSEC Practitioner has determined that certain risks associated with vulnerabilities and indicators are unacceptable and must be mitigated through countermeasures.

3.1.5. Countermeasures.

3.1.5.1. Awareness Training. OPSEC Coordinators will provide computer-based training (CBT) for their personnel and will ensure that the critical information list, threat information, and list of countermeasures in the form of an OPSEC SOP (provided after contract award as Annex C) are provided. In addition, they will provide OPSEC program contact information for reporting and feedback.

3.1.5.2. General Countermeasures. In conjunction with OPSEC awareness training, an OPSEC SOP (provided after contract award as Annex D) will be provided to OPSEC Officer(s) for dissemination to contract and subcontract personnel who support the XYZ program, are involved in technical

The SOP/countermeasures will be provided separately to the winners of the contract and to subcontractors which are part of the OPSEC program.

development, and handle critical information. The OPSEC SOP will include the following countermeasures to be applied whenever personnel handle critical information or indicators on the critical information list:

- Secure electronic transmission and storage of critical information. Critical information *must be transmitted and stored in accordance with the XYZ SOW and related contractor DD254. If there is a question of conformance or practicability, the XYZ PMO OPSEC Practitioner must be consulted for resolution.*

- Secure storage of hardcopy critical information. *Critical information in hardcopy form must be stored in secure areas and/or containers in accordance with the XYZ SOW and related contractor DD254. If there is a question of conformance or practicability, the XYZ PMO OPSEC Practitioner must be consulted for resolution.*

- Protect information after contract is completed. *Require contractors and subcontractors to return government furnished papers and copies of such papers after contract is completed and agree to protect information from public release, from other unauthorized disclosures such as open discussion and at conferences, and through shred/burn if papers are found at a later date.*

- Disposal of hardcopy critical information. *Critical information must be disposed of by cross-cut shredder or burning. Critical information shall not be disposed of in trash receptacles. If there is a question of conformance or practicability, the XYZ PMO OPSEC Practitioner must be consulted for resolution.*

- Codes and markings. *Eliminate coding or coloring systems that indicate an affiliation with the XYZ program. If there is a question of conformance or practicability, the XYZ PMO OPSEC Practitioner must be consulted for resolution.*

- Public Release. *Pre-publication procedures are established to ensure no public release concerning program information occurs without the prior written approval of the XYZ PMO OPSEC Practitioner. OPSEC Officers and Coordinators must be part of any corporate website development and pre-pub review related to the XYZ program, and they must coordinate information related to the XYZ Program with the XYZ PMO OPSEC Practitioner. Critical information is prohibited from being posted on company websites, in blogs, emails, professional journals, research papers, conference presentations, resumes, newsletters, annual reports, etc., without a review. This guidance will be provided as part of the OSPEC SOP. 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 the LSI or next level OPSEC Coordinator for approval by the XYZ PMO OPSEC Practitioner prior to releasing the material.

- Subcontractor Flowdown of OPSEC. *Subcontractors' Statements of Work/contracts will include OPSEC requirements according to this OPSEC Plan, if the contract supports the XYZ technical development and if critical information is involved.*

- Visitor Control. *All visitors are required to process through established checkpoints for verification of identity, citizenship, personnel security clearances (for classified visits), 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 Procedures. *Escorts for visitors shall be advised of proper escort procedures, limitation on disclosure, and other applicable controls involved in the visit.*

- Unauthorized Personnel. *Program personnel shall be alerted when visitors or other unauthorized personnel are admitted to work areas. Personnel shall refrain from 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.*

- Conference Rooms. During meetings, attendees will be reminded of conference room procedures to be followed when discussing critical information. These will include attendance control and procedural security measures (e.g., instructions on note taking and document markings, ensuring protection during breaks, and removal and proper protection after meetings end). When warranted for especially sensitive discussions, secure conference rooms may be used.

3.2. Roles and Responsibilities.

3.2.1. **OPSEC Officer(s).** The OPSEC Officer(s) is located at the LSI.

3.2.1.1. The XYZ PMO OPSEC Practitioner will ensure that the OPSEC Officer(s) will complete OPSEC training to develop skills, which may include the following:

- Threat assessment;
- Identification of critical information;
- Identification of OPSEC indicators;
- Analysis of OPSEC vulnerabilities;

- Assessment of risk;
- Countermeasures development and implementation;
- Contingency and emergency planning; and,
- Awareness training development and presentation.

Training may be computer-based (CBT) or delivered via instructor-led briefing during normally scheduled program meetings.

3.2.1.2. The XYZ PMO OPSEC Practitioner will provide to the OPSEC Officer(s): the XYZ OPSEC Plan with annexes and updates (critical information list, threat information, vulnerabilities, and the OPSEC SOP (countermeasures)), awareness training software, and/or other awareness materials, as appropriate.

3.2.1.3. The OPSEC Officer(s) will ensure that all LSI employees working in support of the XYZ program, involved in the technical development, and handling critical information receive OPSEC awareness training, threat information, vulnerability information, critical information, vulnerability information, and the OPSEC SOP (Countermeasures). The OPSEC Officer(s) will maintain employee training records which must be made available if they are requested from the XYZ PMO OPSEC Practitioner.

These are the main requirements for the contractor workforce, and the heart of the OPSEC program at each level.

3.2.1.4. The OPSEC Officer(s) will ensure that all LSI contracts (subcontract level) that support the XYZ program, involved with technical development and the handling of critical information will include OPSEC requirements in accordance with this OPSEC Plan, as well as a requirement for a flow down in all tier one and below subcontracts that support the XYZ program and are involved in the technical development and handling of critical information.

Subcontract flowdown.

3.2.1.5. The OPSEC Officer(s) will disseminate documentation and materials to the OPSEC Coordinators. The OPSEC Officer(s) will ensure that OPSEC Coordinators at the subcontract level are replaced should the assigned person be unable to participate due to extended illness, extended travel requirements, or reassignment.

3.2.1.6. The OPSEC Officer(s) will ensure that any OPSEC issues that are identified by LSI personnel or those communicated to him/them by the OPSEC Coordinators are provided to the XYZ PMO OPSEC Practitioner. These may include the identification of potential critical information items, vulnerabilities, and/or countermeasures that may need to be addressed.

Feedback loop.

3.2.2. **The OPSEC Coordinators.** Each subcontract that supports the XYZ contract, involves XYZ technical development, and requires the handling of critical information will have an OPSEC Coordinator.

3.2.2.1. The OPSEC Coordinators will successfully complete computer-based OPSEC training (CBT). In addition to that training, OPSEC Coordinators should receive threat information, an critical information list, vulnerability information and the OPSEC SOP from the OPSEC Officer(s) or from their superior OPSEC Coordinator.

3.2.2.2. OPSEC Officer(s) or the superior OPSEC Coordinator will provide to the OPSEC Coordinators: OPSEC guidance, OPSEC Plan with annexes and updates (critical information list, threat information, vulnerabilities, and OPSEC SOP (countermeasures)), awareness training software, and/or other awareness materials, as appropriate.

Subcontract flowdown.

3.2.2.3. The OPSEC Coordinators will ensure that employees in their company who support the XYZ contract, are involved in the technical development, and handle critical information receive computer-based OPSEC awareness training (CBT), threat information, vulnerability information, critical information and the OPSEC SOP (Countermeasures). The OPSEC Coordinators will maintain employee training records which must be made available if they are requested from the XYZ PMO OPSEC Practitioner, the OPSEC Officer(s) or the superior OPSEC Coordinator.

These are the main requirements for the subcontractor workforce, and the heart of the OPSEC program at each level.

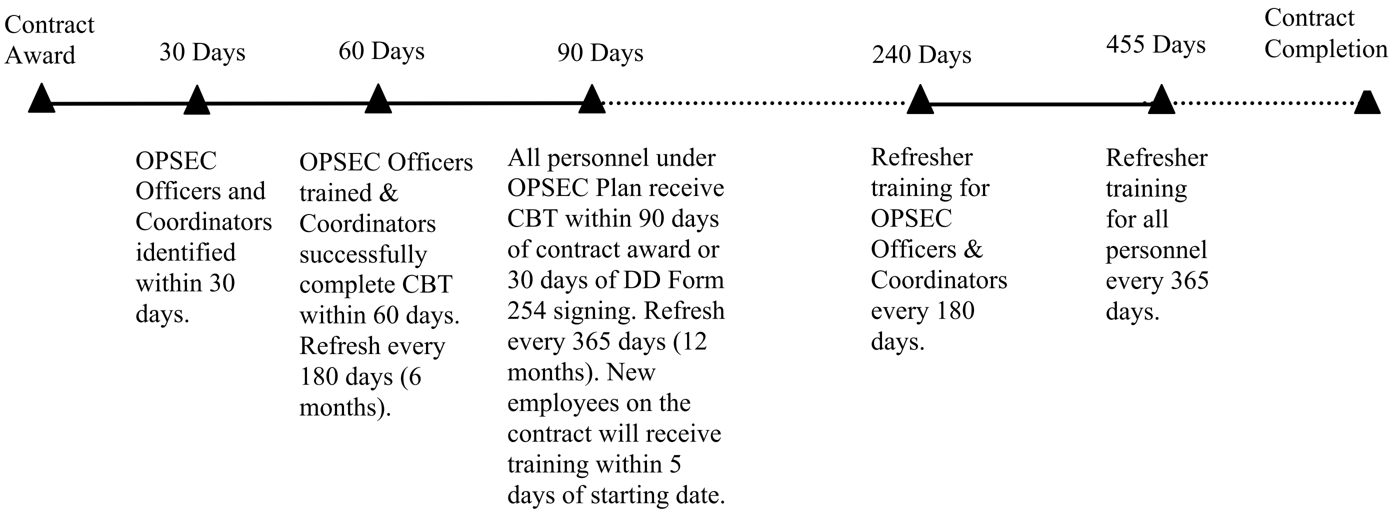
3.2.2.4. The OPSEC Coordinators will ensure that contracts which support the XYZ program, are involved in technical development, and handle critical information will include OPSEC requirements, in accordance with this OPSEC Plan; in addition, they will disseminate documentation and materials to the OPSEC Coordinators at the subordinate subcontractor level and will ensure that these subordinate OPSEC Coordinators are replaced should the assigned person be unable to participate due to extended illness, extended travel requirements, or reassignment.

Continued subcontract flowdown to lower tiers.

3.2.2.5. The OPSEC Coordinators will ensure that any OPSEC issues that are identified by their personnel or those communicated to him/them by subordinate OPSEC Coordinators are provided to the OPSEC Officer(s) at the LSI or to their superior OPSEC Coordinator. These issues may include the identification of potential critical information items, vulnerabilities, and/or countermeasures that may need to be addressed.

Feedback loop.

3.3. Schedule. The OPSEC Officer(s) and OPSEC Coordinators shall follow this schedule:



OPSEC Officers and Coordinators identified within 30 days.

OPSEC Officers trained & Coordinators successfully complete CBT within 60 days. Refresh every 180 days (6 months).

All personnel under OPSEC Plan receive CBT within 90 days of contract award or 30 days of DD Form 254 signing. Refresh every 365 days (12 months). New employees on the contract will receive training within 5 days of starting date.

Refresher training for OPSEC Officers & Coordinators every 180 days.

Refresher training for all personnel every 365 days.

3.2.2.1. The OPSEC Officer and OPSEC Coordinators will be identified within 30 days of contract award.

3.2.2.2. The OPSEC Officer(s) will receive OPSEC training within 60 days of contract award, as determined by the XYZ PMO OPSEC Practitioner. They will receive refresher training every 180 days (six months). Refresher training may be computer-based (CBT) or delivered via an instructor-led briefing during normally scheduled program meetings. New employees on the contract will receive training within 5 days of starting date.

3.2.2.3. The OPSEC Officer(s) will ensure that personnel working at the LSI and at the subcontractor levels who are working in support of the XYZ program, are involved in the technical development, and handle critical information will receive computer-based OPSEC awareness training (CBT) within 90 days of contract award or within 30 days of the signing of the DD Form 254. Training will be repeated every 365 days (12 months). It is estimated that 75% of all personnel who are working on contracts that support the XYZ program who are involved in the technical development will be handling critical information.

4. Statement of Conformance:

I, ___________________________, am representing ___________________________________, and agree to conform to the requirements of this Operations Security Plan. If conformance cannot be achieved, I will provide a statement of non-conformance within 15 days after receiving the critical information list and the OPSEC SOP.

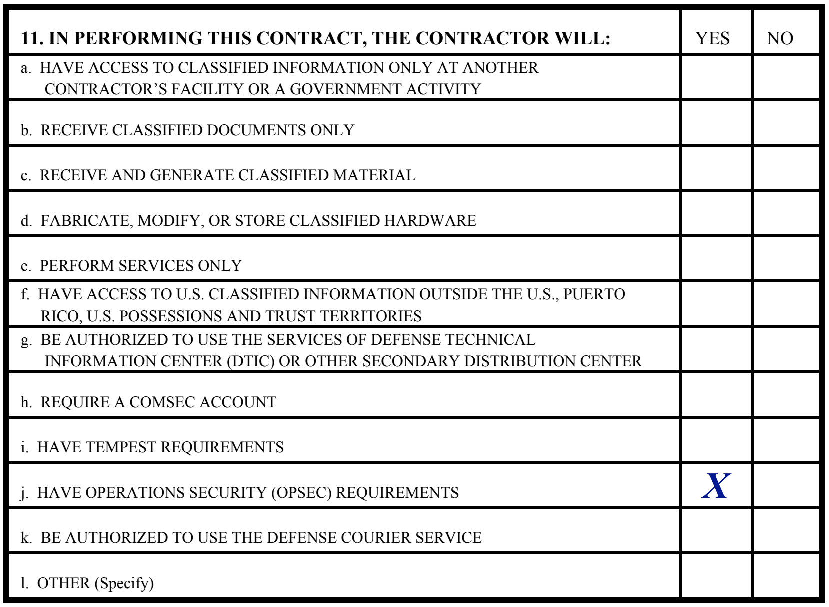
Signature: ______________________________ Date: _____________

Title: __________________________________

We recommend including OPSEC as one of the criteria in the proposal evaluation process. However, we realize that this is not always possible, and in those cases we recommend that a statement of conformance be included with the contractual OPSEC plan. Once the contract is awarded, the contractor must sign the statement of conformance and then notify the Government sponsor if additional issues arise in the future. This statement must be included in all subcontracts where the OPSEC plan is relevant.

D. Classified Contracts and the DD Form 254 (Department of Defense Contract Security Classification Specification)

According to the DSS Academy (DSSA) pamphlet entitled, “A Guide for the preparation of the DD Form 254,” the Federal Acquisition Regulation (FAR) requires that a DD Form 254 be incorporated in each classified contract, and the National Industrial Security Operating Manual (NISPOM) (4-103a) requires that a DD Form 254 be issued by the Government with each Invitation for Bid, Request for Proposal, or Request for Quote. The DD Form 254 provides to the contractor (or a subcontractor) the security requirements and the classification guidance that would be necessary to perform on a classified contract. (The IOSS recommends this pamphlet, which was created to assist Government contracting personnel and prime contractors in their preparation of a DD Form 254. It contains step-by-step procedures for filling out the form.) This pamphlet is very useful and we have modified sections pertaining to OPSEC to help your DD Form 254 correspond to your contractual documents and provide clarity to the contractor.



11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR’S FACILITY OR A GOVERNMENT ACTIVITY		
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		
e. PERFORM SERVICES ONLY		
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		
h. REQUIRE A COMSEC ACCOUNT		
i. HAVE TEMPEST REQUIREMENTS		
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	*X*	
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		
l. OTHER (Specify)		

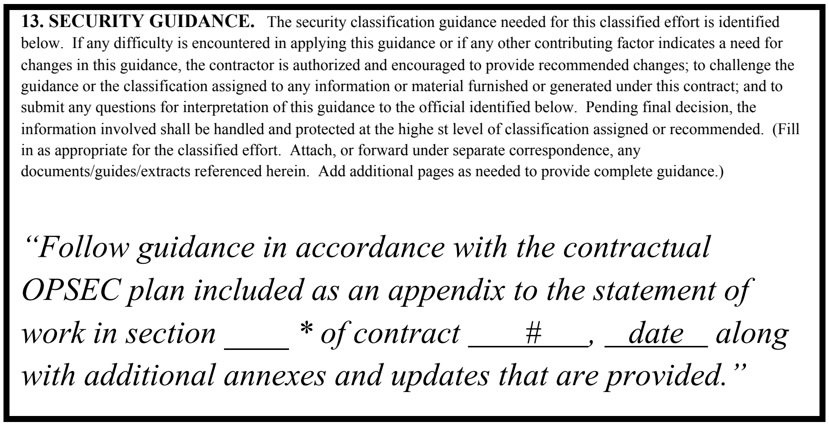
1. Item 11.j. “Have Operations Security (OPSEC) Requirements”

Mark “YES” if the contractor must impose certain countermeasures directed to protect critical information.

2. Items 13 and 14. “Security Guidance” and “Additional Security Requirements”

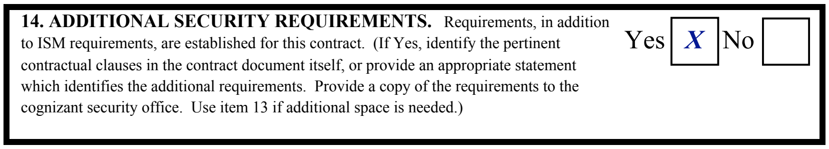
According to the DSSA pamphlet, “OPSEC requirements are additional to the requirements of the NISPOM. Thus, contractors may not impose OPSEC requirements on their subcontractors unless the [government sponsor of the contract] approves the OPSEC requirements.” Also, “If marked “YES,” Item 14 must also be marked “YES” and pertinent contract clauses identified or added to Item 13.”

We recommend a statement such as the following be included in block 13 (or 14), *"Follow guidance in accordance with the contractual OPSEC plan included as an appendix to the statement of work in section ____ * of contract ____#____, __date__ along with additional annexes and updates that are provided."*


13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highe st level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

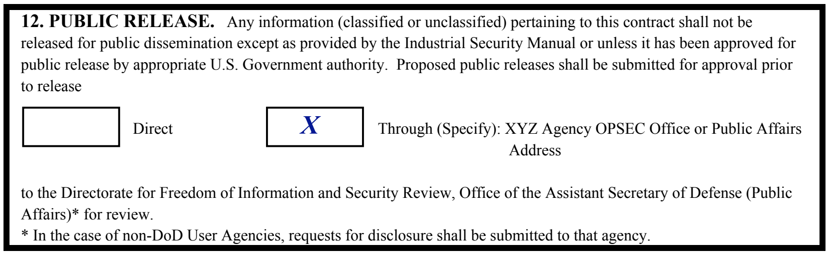
*"Follow guidance in accordance with the contractual OPSEC plan included as an appendix to the statement of work in section ____ * of contract ____#____, __date__ along with additional annexes and updates that are provided."*

*Note: The statement and the section of the contract will be specified by your organization's contracting personnel.


14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use item 13 if additional space is needed.) Yes ☒ No □

3. Item 12. "Public Release"

The DD Form 254 provides an additional OPSEC countermeasure in item 12 for public release. We recommend you check the "through" box and list your office or the public affairs office to ensure there is an OPSEC review of all the contractor's public releases regarding this contract. By doing so, you ensure that advertising and other releases do not give away critical information.


12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release

□ Direct ☒ Through (Specify): XYZ Agency OPSEC Office or Public Affairs Address

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
* In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

IV. Resources

A. Threat Information

- DSS, *Technology Collection Trends…*
- IOSS, *Intelligence Threat Handbook*
- FBI *ANSIR, Infragard, Domain Coordinator*
- Society of Competitive Intelligence (SCIP)
- ONCIX, Annual Report to Congress on Foreign Economic Collection and Industrial Espionage

B. Awareness

- CBT: "*An Introduction to OPSEC*" (IOSS' OPSEC primer)
- www.ioss.gov
- www.dss.mil

C. OPSEC in Contracts

- "Operations Security: Placing OPSEC on Contracts," 2007, Teresa Anderson, Operations Security Office, Wright-Patterson Air Force Base (WPAFB)

- "Contracting Operations Security (OPSEC) Handbook," 2002, 88th Security Forces Squadron (WPAFB) www.asc.wpafb.af.mil.sfs/sfa/opsec.htm *Future: Handbook on OPSEC in Contracts*

- Defense Acquisition University (DAU) Continuous Learning Module CLC 107 "OPSEC Contract Requirements" www.dau.mil

- "A Guide for the preparation of the DD Form 254," Defense Security Service Academy (DSSA)

D. Policy

- NSDD 298
- DoD OPSEC Program Directive 5205.2
- Industrial Security Regulation 5200.22R
- National Industrial Security Manual (NISPOM) Supplement 5200.22M-Sup 1