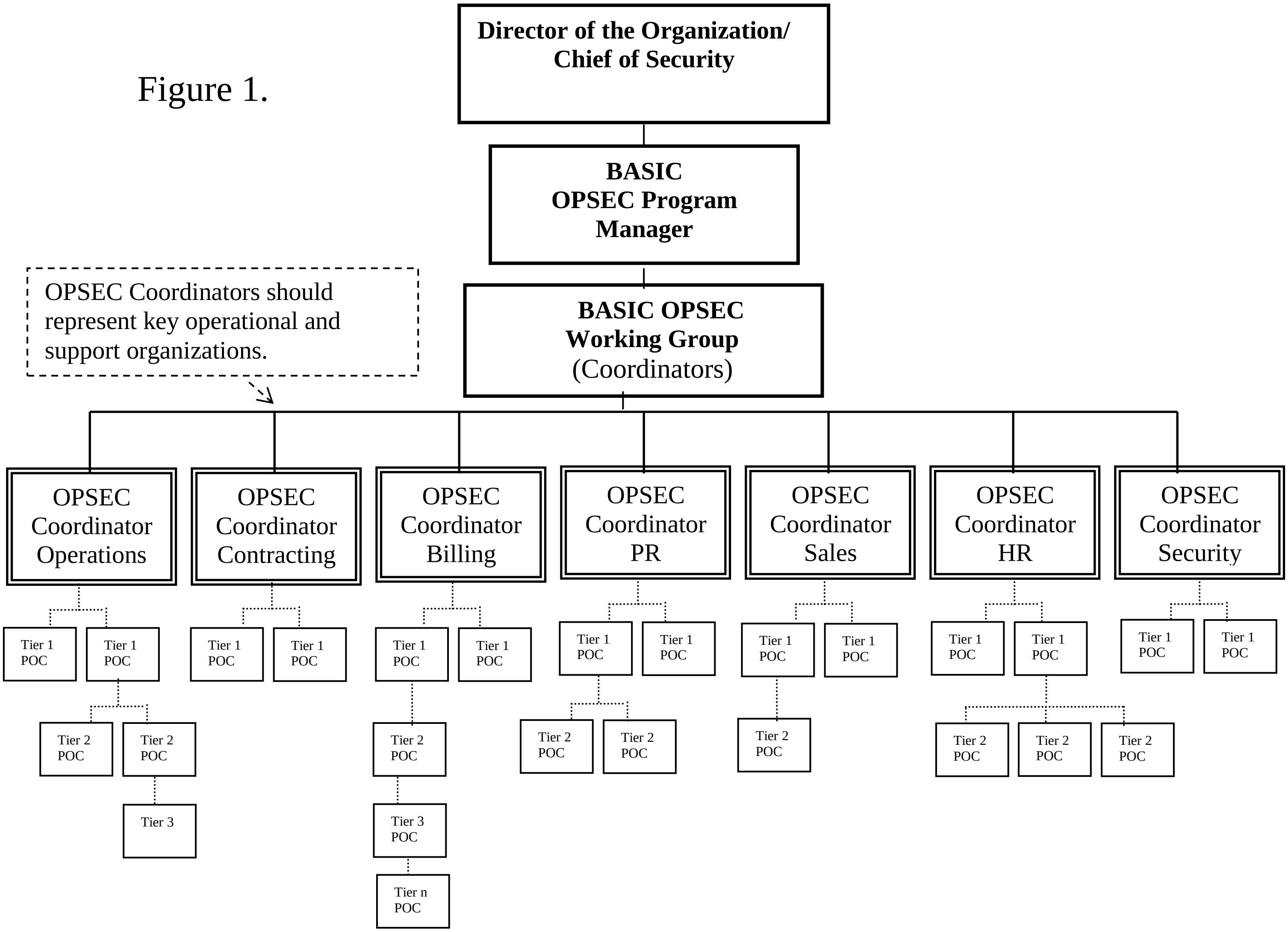
BASIC OPERATIONS SECURITY (OPSEC) PLAN
DAY MONTH YEAR

1. PURPOSE: The BASIC OPSEC Program will provide the structure needed to offer OPSEC guidance and support to BASIC operations worldwide, conduct and/or support OPSEC assessments, and recommend improvements. The program will also:

- Provide an analytic process to identify critical information.
- Assist in identifying cost-effective countermeasures that will close vulnerability gaps and lower risk to operations and activities worldwide.
- Ensure that the number one vulnerability – lack of awareness – is countered through effective, regular and mandatory OPSEC Awareness training.

2. ORGANIZATION: This OPSEC Program and its requirements apply to all BASIC personnel who will participate in the OPSEC program under the following management structure (see Figure 1):

Figure 1.


Director of the Organization/ Chief of Security
BASIC OPSEC Program Manager
BASIC OPSEC Working Group (Coordinators)
OPSEC Coordinators should represent key operational and support organizations.
OPSEC Coordinator Operations
OPSEC Coordinator Contracting
OPSEC Coordinator Billing
OPSEC Coordinator PR
OPSEC Coordinator Sales
OPSEC Coordinator HR
OPSEC Coordinator Security
Tier 1 POC
Tier 2 POC
Tier 3
Tier 3 POC
Tier n POC

3. Roles and Responsibilities.

3.1 OPSEC Program Manager. The BASIC OPSEC Program Manager is responsible for developing the OPSEC Plan and monitoring its implementation and operation to ensure compliance. He serves as the principal advisor to the Chief of the Organization and/or Chief of Security on all OPSEC matters and will:

1) Coordinate all OPSEC policy responsibilities and procedures within the program.

2) Revise the OPSEC Plan as necessary, including the critical information lists, threat assessment, vulnerabilities, risk, and countermeasures.

3) Accumulate and disseminate updated threat information and awareness materials to program personnel.

5) Assist in the review of contract requirements for OPSEC considerations.

6) Ensure that the OPSEC Coordinators and selected POCs will complete OPSEC training to develop skills, which may include the following:

- Threat assessment;
- Identification of unclassified 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 briefings.

7) The BASIC PMO OPSEC Program manager will provide to the OPSEC Coordinators: the BASIC OPSEC Plan with generally written annexes and updates (unclassified critical information list, threat information, vulnerabilities, and the OPSEC SOP (countermeasures)), awareness training software, and/or other awareness materials, as appropriate. Critical Information Lists, threat, vulnerability and countermeasures should be coordinated with personnel from the lowest possible tier to ensure effectiveness.

3.2. OPSEC Coordinators. The OPSEC Coordinators will successfully complete OPSEC training. The role of the OPSEC coordinator is to provide OPSEC oversight for the lower tier levels and to interface with the OPSEC Program Manager to elevate issues that affect BASIC at large. OPSEC Coordinators will be responsible for awareness training, identification of critical information lists and countermeasures, other OPSEC issues and vulnerabilities, and implementation of OPSEC policies and procedures, and will work through OPSEC Points of Contact (POCs) who are identified in lower tiers of the company. The OPSEC Coordinators will maintain employee training records which must be made available if they are requested from the BASIC OPSEC Program Manager. They will ensure that any OPSEC issues that are identified by OPSEC POCs or personnel are provided to the BASIC OPSEC Program Manager. These may include the identification of potential unclassified critical information items, vulnerabilities, and/or countermeasures that may need to be addressed.

3.3. OPSEC Working Group. The role of the OPSEC working group is to ensure the BASIC OPSEC Program implementation is consistent across the organization, and is integrated at the working level. The working group will also assist the OPSEC Program Manager to develop general countermeasures and solutions. The working group will provide coordination of all recommendations being forwarded to senior leadership, and will assist with development of briefings and reports.

4. POLICY: All mandated areas in the company will participate in the OPSEC program.

4.1. All personnel will receive OPSEC orientation training within [30/60/90] days of assignment. OPSEC coordinators will conduct initial orientation training using materials provided by the OPSEC program manager.

4.2. All personnel will participate in [annual/biannual/quarterly/monthly] OPSEC awareness training. Coordinators will ensure that attendance for all personnel in their department is documented, and will provide a memo to that effect to the OPSEC Program Manager within [10/30] days of the training.

4.3. The OPSEC Program Manager will participate as an emergency actions team member, and will provide appropriate OPSEC analysis support and countermeasures recommendations.

4.4. The OPSEC Program Manager will brief the Chief of the Organization on OPSEC issues and changes to the intelligence threat [periodically/weekly/monthly/quarterly].

4.5. Each company department will provide a senior representative to the OPSEC working group. Managers will ensure the working group representative is replaced should the assigned person be unable to participate due to extended illness, extended travel requirements, or reassignment. Working group members will attend training as determined by the OPSEC program manager.

4.6. Each [division/branch/functional area] will provide one or more OPSEC coordinators depending on size and responsibilities of each element. The OPSEC Program Manager will ensure that the OPSEC coordinator is replaced should the assigned person be unable to participate due to extended illness, extended travel requirements, or reassignment. OPSEC coordinators will attend training as determined by the OPSEC program manager. OPSEC coordinators will provide reports, assist with orientation and awareness training, and perform other OPSEC functions as determined by the OPSEC program manager.

4.7. All personnel will be familiar with the critical information list for their department or program, and will be prepared to describe appropriate OPSEC countermeasures they can apply to protecting that information in accordance with their awareness training.

5. REQUIREMENTS:

5.1. OPSEC Process.

5.1.1. Unclassified critical information. An unclassified critical information list and updates will be provided under separate cover (Annex A) to the OPSEC Coordinators for dissemination to employees in their respective department. For maximum effectiveness, the critical information list should be developed at the lowest possible tier.

5.1.2. Threat Assessment. Capable adversaries collecting unclassified, as well as classified, information on BASIC and companies developing similar technologies may pose a threat to the BASIC company, its employees, customers, partners and vendors. A formal threat assessment and all updates will be provided under separate cover (Annex B) to the OPSEC Coordinators for dissemination to OPSEC POCs in lower tiers, as necessary. A general threat assessment is provided below.

5.1.2.1. 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 actually increased dramatically in recent years.

5.1.3. Vulnerability Analysis. Vulnerabilities (and indicators) of the program may reveal unclassified critical information. A general and contractual vulnerability analysis is provided below.

5.1.3.1. 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-unclassified 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, 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.

- *Professional Conferences/Symposia.* Company 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.

- *Contracting.* Companies may fail to recognize the need for the imposition of OPSEC requirements in contracts and subcontracts.

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

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

- *Disgruntled Employees and Employees with Personal Problems.* Personnel possessing security clearances may, 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 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.

5.1.3.2. Contractual Vulnerability Analysis. The following contractual vulnerabilities are most commonly identified in OPSEC assessments:

- Use of an external travel office; travel patterns, and travel practices;
- Geographic separation of various corporate locations;
- Sympathies of 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 international partners and subcontractors; and,
- Unauthorized access to specific unclassified performance parameters related or identified with the program.

5.1.4. Risk Assessment. The BASIC OPSEC Program Manager has determined that certain risks associated with vulnerabilities and indicators are unacceptable and must be mitigated through countermeasures.

5.1.5. Countermeasures.

5.1.5.1. Awareness Training. OPSEC Coordinators will provide computer-based training (CBT) or briefings for their personnel and will ensure that the unclassified critical information list, threat information, and list of countermeasures in the form of an OPSEC SOP (Program Plan Annex C or one tailored to the department) are provided to personnel and/or OPSEC POCs. In addition, they will provide contact information for reporting and feedback.

5.1.5.2. General Countermeasures. In conjunction with OPSEC awareness training, an OPSEC SOP (OPSEC Plan Annex C or one to tailored to the department) will be distributed to personnel and/or OPSEC POCs. The OPSEC SOP will include the following general countermeasures to be applied whenever personnel handle unclassified critical information or indicators on the unclassified critical information list:

- *Secure electronic transmission and storage of unclassified critical information. Unclassified* critical information must be transmitted and stored in accordance with the OPSEC SOP. If there is a question of conformance or practicability, the BASIC OPSEC Program Manager must be consulted for resolution.

- *Secure storage of hardcopy unclassified critical information.* Unclassified critical information in hardcopy form must be stored in secure areas and/or containers in accordance with the OPSEC SOP. If there is a question of conformance or practicability, the BASIC OPSEC Program Manager must be consulted for resolution.

- *Disposal of hardcopy unclassified critical information.* Unclassified critical information must be disposed of by cross-cut shredder or burning. Unclassified critical information shall not be disposed of in trash receptacles. If there is a question of conformance or practicability, the BASIC OPSEC Program Manager must be consulted for resolution.

- *Codes and markings.* Eliminate coding or coloring systems that indicate an affiliation with the BASIC company, posing an unacceptable risk. If there is a question of conformance or practicability, the BASIC OPSEC Program Manager must be consulted for resolution.

- *Public Release.* Pre-publication procedures are established to ensure no public release concerning company information occurs without the prior written approval of the BASIC OPSEC Program Manager. The OPSEC Program Manager must be part of any corporate website development and pre-pub review related to the BASIC company, unless delegated to the OPSEC Coordinators. Unclassified 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. Contractors and subcontractors are required to forward all material for public release through the OPSEC Program Manager and/or

Coordinators for approval by the BASIC OPSEC Program Manager prior to releasing the material.

- *Contractor/subcontractor Flowdown of OPSEC.* As appropriate, and if unclassified critical information is involved, contractors and subcontractors' Statements of Work/contracts will include OPSEC requirements according to this OPSEC Plan.

- *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.* 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 unclassified 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.