(Organization) OPERATIONS SECURITY (OPSEC) PLAN
(Date)

1. **PURPOSE**: This OPSEC plan will provide the structure needed to offer OPSEC guidance and support to (organization). It specifically addresses threat, critical information, vulnerabilities and risks, and necessary OPSEC measures to protect the (organization) mission.

2. **THREAT**: Capable adversaries collect unclassified information on (organization). A formal threat assessment is available under separate cover. The worldwide intelligence collection threat is comprised of multi-disciplined, highly sophisticated, and extremely dedicated adversaries. Their collection efforts potentially target all DoD operations, especially those related to a mission or operation closely related to one of their primary intelligence requirements. (Add relative local data)

3. **CRITICAL INFORMATION (CI)**: CI is that information that an adversary would need to interfere with friendly activities or operations, or to be successful in their mission. The CI list should also include any information uniquely essential to friendly objectives. Understanding the adversary and their information requirements is essential to correctly identifying CI. (Add relative local data)

4. **VULNERABILITIES AND RISK**: Vulnerabilities are those situations or conditions that make (organization) susceptible to intelligence collection. Each vulnerability has an associated level of risk; the senior person associated with a mission should make a determination of acceptable levels of risk. (See DODM 5205.02-M has detailed instructions on estimating risk levels.) The most significant vulnerabilities associated with the (organization) mission are: (delete those below that don’t apply; add others as appropriate.)

4.1. 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. Risk: (provide an estimate of risk based on the value of CI that could be susceptible due to this vulnerability and the impact should this vulnerability allow the adversary to exploit CI)

4.2. 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. Risk: (provide an estimate of risk based on the value of CI that could be susceptible due to this vulnerability and the impact should this vulnerability allow the adversary to exploit CI)

4.3. Staff use of Social Media. Social media are a unique form of web page, and represent a higher level of risk because they are designed specifically for people to share information. Adversaries exploit social media by using them to target individuals, by using social engineering to elicit information, and to gather intelligence. Risk: (provide an estimate of risk based on the value of CI that could be susceptible due to this vulnerability and the impact should this vulnerability allow the adversary to exploit CI)

4.4. 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. Risk: (provide an estimate of risk based on the value of CI that could be susceptible due to this vulnerability and the impact should this vulnerability allow the adversary to exploit CI)

4.5. 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. Risk: (provide an estimate of risk based on the value of CI that could be susceptible due to this vulnerability and the impact should this vulnerability allow the adversary to exploit CI)

4.6. Visitor Control. Visitors within the facility may observe or overhear unclassified critical information regarding operations, activities, etc. Risk: (provide an estimate of risk based on the value of CI that could be susceptible due to this vulnerability and the impact should this vulnerability allow the adversary to exploit CI)

4.7. Conference Room Security. Unclassified critical information can be compromised if there are no procedures in place to control discussions. Risk: (provide an estimate of risk based on the value of CI that could be susceptible due to this vulnerability and the impact should this vulnerability allow the adversary to exploit CI)

5**. POLICY:** Members of (organization) will to the greatest extent possible use the following OPSEC measures to mitigate unacceptable risks.

5.1. All personnel will receive OPSEC orientation training within [30/60/90] days of assignment.

5.2. All personnel will participate in [annual/biannual/quarterly/monthly] OPSEC awareness training.

5.3. All personnel will be familiar with the (organization) critical information list.

5.4. Add other appropriate OPSEC measures. The following may apply:

- *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.

- *Public Release.* Pre-publication procedures are established to ensure no public release without prior written approval Reviews should be conducted on announcements concerning visits, tests, and activities posted within facilities about program matters.

- *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.