STATEMENT OF WORK: OPERATIONS SECURITY (OPSEC) REQUIREMENTS

1. As defined in Army Regulation (AR) 530-1, Operations Security (OPSEC), sensitive information is information requiring special protection from disclosure that could cause compromise or threat to our national security, an Army organization, activity, family member, DA civilian or DoD contractor. Critical Information is defined as information important to the successful achievement of U.S. objectives and missions, or which may be of use to an adversary of the United States. It consists of specific facts about friendly capabilities, activities, limitations (includes vulnerabilities), and intentions needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishment. All critical information is sensitive, but not all sensitive information is critical.

2. The Contractor shall not release sensitive information to the general public without prior written approval from the Contracting Officer. All contractor requests to release sensitive information shall be in writing and clearly explain the necessity for release of the information and consequences if approval is not granted. Contractor employees who are U.S. citizens shall be provided access to sensitive information on a "need to know" basis required to fulfill the terms and conditions of the contract. Foreign National (FN) employees' access to information will be limited to non-sensitive information. FN access to sensitive information will be approved in writing by the Contracting Officer on a case-by-case basis, and will be strictly limited to the information that the employee must know in order to fulfill the terms and conditions of the contract.

3. The Contracting Officer will provide the Contractor with a list of known Critical Information (CI) pertinent to contract requirements as soon as possible after contract award. Critical Information shall be used by the Contractor's appointed OPSEC Manager to prepare an OPSEC Plan.

4. The Contractor shall be responsible for establishing and maintaining an OPSEC program to adequately manage, protect and control sensitive information that has been provided or generated under the contract. The Contractor shall prepare and submit a written OPSEC Plan to the Contracting Officer for approval IAW DD 1423/DI-MGMT-80934C within 30 calendar days after receipt of the CI information addressed in Paragraph 3 above. The Contracting Officer will coordinate with the Government OPSEC Officer and advise the Contractor in writing of the approval, conditional approval or disapproval of the plan within 20 days of receipt.

5. The Contractor shall conduct annual self-assessments of their OPSEC program and submit annual written assessments to the Contracting Officer in the anniversary month of contract award. OPSEC Assessment checklists and sample assessment responses will be provided in advance by the Government as tools to aid the Contractor in assessing their OPSEC program.

6. The Contractor shall provide OPSEC training to all employees regarding the safeguarding of sensitive information prior to employees being allowed access to such information, and annually thereafter.

7. The Contractor shall destroy all sensitive program material at the completion of the contract so as to ensure the information cannot be accessed or utilized for any purpose and notify the Contracting Officer in writing of its destruction.

8. These same requirements will flow down to all subcontractors working on or provided any sensitive information related to the contract.

END STATEMENT OF WORK