Operations Security (OPSEC) Guide for Defense Contractors

Developed by:

EM/Security Office
U.S. Army Corps of Engineers
Fort Worth District
Fort Worth, TX
76102-0300

REVISION HISTORY

Revision	Date	Summary of Changes
N/A		Original issue
N/A	14 Feb 2019	Reviewed/updated

TABLE OF CONTENTS

Page

Ref: (a) National Security Decision Directive Number 298, National Operations Security Program
(b) DoDINST 5205.02-M, Department of Defense Operations Security Program
(c) DoDINST 5220.22M, National Industrial Security Program Manual (NISPOM)
(d) AR 530-1, Army Regulation Operations Security
(f) U.S. Army Corps of Engineers, Fort Worth District, Operations Plan, August 2018
(g) Interagency OPSEC Support Staff Publication; Applying OPSEC to Government Contracts
(h) U.S. Army Corps of Engineers, Fort Worth District Critical Information List
(i) Federal Acquisition Regulations (FAR)
(j) Defense Federal Acquisition Regulation Supplement (DFARS)

1. Purpose. This document provides Operations Security (OPSEC) guidance to Government Contractors, e.g; corporations and businesses and independent contractors awarded government work for U.S. Army Corps of Engineers, Fort Worth District (SWF) and at SWF projects at other Army facilities and installations. Government Contractors are provided this guidance to ensure compliance and protection of Nation Security Information.

2. Definition. OPSEC is an analytical process to identify Critical Information (CI), identify threats to that Critical Information and the related vulnerabilities and risks of exploitation to that CI, and identify, develop, and implement countermeasures to protect that CI. CI is specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. CI includes those facts, which individually, or in the aggregate, reveal sensitive details about Untied States Government and/or SWF or, the contractor's Security or operations related to the support or performance of the Statement of Work (SOW) or the Performance Work Statement (PWS), and thus require a level of protection from adversarial collection or exploitation not normally afforded to unclassified information. OPSEC supplements, but does not replace traditional security practices such as Physical Security and Information Security. OPSEC is essential to ensure the initial and continued success of our mission, operations, systems, and procedures.

3. OPSEC Applicability. The OPODR 2013-74 has determined that additional safeguards are essential for specific contracts, and imposes OPSEC as a requirement in addition the standard requirements for participation in the National Industrial Security Program Manual (NISPOM). Contractors must adhere to the guidance stipulated in SECTIONS I and/or, II or III below when OPORD 2013-74 specify OPSEC requirements during the performance of work. The government has determined that OPSEC is required during the period of this contract because:

a. The Contractor requires long or short-term physical access to SWF facilities or SWF projects at other Army installations or facilities, therefore the minimum OPSEC requirements specified in Section I apply. This includes but is not limited to:

(1) Contractor personnel who require intermittent or short-term access, such as; construction, installation and repair crews, recurring visitors, some route delivery personnel, those attending multiple meetings, conducting inspections, onsite training, or requiring physical access to other government information systems, on behalf of SWF, (Section I applies) and/or;

(2) Require continuous access, such as ALL embedded contractors, direct support personnel, maintenance and/or janitorial services and those viewing or participating in sensitive operations, (Sections I and II apply) or;

(3) With direct or indirect access to Government CI; Army logistics services, photography, recording, surveying, printing, graphics design, and/or reproduction services of government information or material (Section I and II apply) or;

b. The contract includes U.S. Government supplied material for production of sensitive unclassified material or components including: Tools, Technical Drawings and/or Technical Data, or; Military Critical Technologies List, and/or Dual-Use Technology items, including Commercial Off The Shelf (COTS) technology adapted for specific military applications. Where no there is no specific OPSEC plan or requirements to develop one;

(1) The contractor shall follow all applicable security rules and regulations to protect its proprietary information and that of the government. Public release or release to third parties of government information provided is not authorized with government approval. Contact SWF Public Affairs Officer and SWF Security Office.

c. The Contract is for production of items which may have an established OPSEC plan or; Program Protection Plans and/or; when a contract includes or develops Critical Information. Therefore the minimum OPSEC requirements specified in Section III apply.

(1) OPSEC is usually required in system acquisition (e.g. weapon systems, electronic countermeasures, radio transmitters, active sensors, or low observable capabilities) or sensitive activities (such as intelligence operations or testing of foreign materials), particularly if such contracts involve special access.

(2) The contractor may use or produce, U.S. Government Critical Information (CI) and/or Observables and Indicators which may lead to discovery of CI. In which case basic OPSEC Awareness and measures should be implemented

d. In cases where this is question as to the proper application of elements of this guide, the SWF OPSEC Officer should be consulted. Deviation from this guidance is not authorized without approval. The SWF OPSEC Officer can be reached at (817) 886-1442. The SWF OPSEC Officer will provide a list of SWF critical information to be protected.

I. GENERAL CONTRACTOR OPSEC REQUIREMENTS

During the course of this contract, in addition to those restrictions, instructions and guidelines delineated in the contract SOW/PWS and/or other references provided, the contractor will adhere to the following minimum requirements in support of OPODR 2013-74:

a. Introduction of personnel electronic devices into government spaces, laptops, tablet PCs, cellular phones, cameras, recording devices, and data recording/storage devices is STRICTLY controlled and forbidden in most cases. Company issued equipment required for the performance of work must be approved by the government security officer. Photography and recording is not allowed except for official use and by permit only. (Unless otherwise stipulated in the contract, contact the Installation or SWF Security Officer for approval.)

b. Contractor personnel shall not discuss government operations in public or over unprotected or unencrypted communications. Official Business, controlled unclassified information may only be transmitted as directed in the SOW/PWS.

c. The Contractor shall not post to company websites, publications, newsletters or other media any images, data or information that reveal sensitive government operations, personnel, equipment, and/or classified or controlled unclassified information, refer to paragraph (d) below. When in doubt, company press releases related to this contract should be coordinated through the SWF Public Affairs Officer. The SWF Public Affairs Officer will approve all public releases of information on SWF contracts.

d. Contractor personnel shall not disclose to unauthorized third parties, post to unofficial sites (including all Social Networking sites) any images, data or information that reveals sensitive government operations, personnel, equipment, including, but not limited to:

(1) Tactics, techniques and procedures, production or work schedules, any visible or concealed modifications, upgrades, additions to Army installations, property or weapons or equipment; increases, change, or decreases in work/deployment frequency or government personnel, project schedules, logistics or material delivery schedules; specialized equipment orders, deliveries, shipments, etc. (Unauthorized disclosure and transfer of National Security Information is punishable under 18 USC § 793.)

(2) Non-Disclosure requirements remain in effect during the duration of this contract an indefinitely thereafter.

(3) Unauthorized disclosures and attempts to solicit this type information by unauthorized third parties or others not affiliated with this contract shall be reported to the SWF and/or installation Security Office, our Contracting Officer Representative (COR) contract, and your company Facility Security Officer and/or the Defense Security Service.

e. Government issued CACs, badges, identification shall be removed and/or concealed from plain sight when off station and shall not be left in vehicles or unprotected. Badges and Passes may not be duplicated or copied. Lost or stolen identification badges, vehicle passes etc. will be immediately reported to the COR and/or installation
Security Office.

f. Practice OPSEC and implement countermeasures to protect Critical Information (CI) and other sensitive unclassified information and activities vigilance, or degrade the planning and execution of military operations performed or supported by the contractor in support of the mission. Protection of CI will include the adherence to and execution of countermeasures which the contractor initiates or as provided by SWF OPSEC Officer or installation OPSEC Officer, for CI on or related to the SOW/PWS.

g. The contractor must mark and protect related internal production schedules, deliverables, inventories and shortages and identified vulnerabilities related to production of government material as For Official Use Only Information in accordance with guidance in paragraphs C121 and/or C115 (If applicable) of this SOW.

h. All government information must be destroyed at contract termination or returned to the government at the government's discretion

Permanent Onsite Contractors: Where a contract includes permanent/embedded contract personnel at SWF facilities or on other Army installations, these additional requirements apply:

(1) Assign an OPSEC Point of Contact for this contract.

(2) OPSEC Awareness Education and Training will be provided or coordinated through government channels as a cost management process. All personnel supporting the contract will receive initial OPSEC awareness training and Annual OPSEC Refresher training; contact the SWF COR or SWF Operations Security Officer to assist in this requirement.

(2) CI listed below and that listed in the SWF Command Critical Information List (CIL) or additional information identified by our Contracting Officer Representative

(COR) including company-generated information whether in electronic or hardcopy form; e.g.; internal schedules, deficiency reports, and other internal documents, related

to this project will be marked and handled appropriately as FOR OFFICIAL USE ONLY (FOUO) or other required marking in accordance with guidance in this SOW/PWS. Government Critical Information includes but is not limited to: Known or probable vulnerabilities to any U.S. system and their direct support systems, Details of information about military operations, Army units, troop movements/arrivals, missions and exercises, etc.

(3) A complete list of Critical Information will be provided to the contractor site manager (if assigned) by the Army installation OPSEC Officer or by the SWF OPSEC Officer. Questions regarding Critical Information shall be directed toward the SWF Program Manager, Project Manager of COR.

(4) OPSEC requirements are additional to the requirements of the NISPOM, reference (b). Thus, contractors may not impose OPSEC requirements on their subcontractors unless SWF approves the OPSEC requirements.

II. OPSEC Training Requirements.

Where a contract requires long term access to SWF or other Army government facilities, such as embedded contractors, onsite work or participates in our operations, they must follow the provisions of the OPORD 2013-74 to include training and awareness.

a. Initial training may be provided by computer-based Training, live training or a combination of both.

b. OPSEC training is required initially within 30 days of assignment and annually thereafter.

c. The contractor is required to maintain individual training records for compliance purposes.

III. Contractor Developed OPSEC Plans.

When a Contractor developed OPSEC Plan is required, the SOW/PSW will include specific contract language and Data Item Descriptor D-MGMT-80934B (Operations Security Plan) will be provided as part of the awards package. The Data Item Descriptor provides specific guidance for developing an OPSEC Plan and will be tailored to include only that information that is necessary to ensure CI is adequately protected. The OPSEC plan must include a program for internal OSPEC training of all employees working on the project.

a. Specific guidance is provided in Section J of the contract solicitation (or award, as applicable), i.e. “Operations Security Plan Requirements.” OPSEC plan requirements must be included for any and all subcontractors. A copy of subcontractor OPSEC Plans must accompany the subcontractor DD254s provided to the SWF Security Officer."

b. Compliance with security requirements imposed by documents generated in response to DoD 5200.39, Critical Program Information (CPI) Protection within the Department of Defense is required. Compliance with OPSEC measures identified in the existing OPSEC Plan for this program is required. The plan will be provided to the SWF Program Manager, Project Manager, COR and SWF OPSEC Officer for review and approval.

c. When an OPSEC plan from the contractor is required, the COR is responsible for obtaining and submitting the contractor's existing or proposed plan to the OPSEC Officer for review. A contract award DD254 will not be endorsed or issued by the Security Office until the SWF OPSEC Officer has approved the contractor's OPSEC plan.

d. If the company has an existing OPSEC Plan, awareness, education, training, and planning processes in place to protect corporate information, these should be applied pending government acceptance rather than creating a new program.

e. OPSEC Awareness Education and Training will be provided or coordinated through SWF public web site as a cost management process. All personnel supporting the contract will receive initial OPSEC awareness training and Annual OPSEC Refresher training as required; contact the SWF Program Manager, Project Manager of COR or the SWF OPSEC Officer to assist in this requirement.

f. Program OPSEC plans shall be coordinated with SWF Program Manager, Project Manager of COR and approved by the SWF OPSEC Officer and shall be imposed on subcontractors as appropriate. Program protection measures shall be applied and approved by SWF Program Manager, Project Manager of COR at ALL locations where Critical Information is developed, produced, analyzed, maintained, transported, stored, tested, or used in training.

g. The contractor should request guidance from the COR on any specific predetermined OPSEC critical information associated with the contract during the preparation of OPSEC plans or any associated OPSEC plans that directly relate to the information provided by the government. OPSEC protective measures will be applied as directed by the SWF Program Manager, Project Manager or COR. While performing on a government site, the contractor shall comply with the OPSEC guidance or plans specific to that location or program supported.

GLOSSARY

CI- Critical Information

CIL- Critical Information List

COMINT- Communications Intelligence

COMSEC- Communications Security

COMPUSEC- Computer Security

COR- Contracting Officer’s Representative

CPI- Critical Program Information

CUI- Controlled Unclassified Information

DoD- Department of Defense

DoA- Department of the Army

DSS- Defense Security Service

EAA- Export Administration Act

EAR- Export Administration Regulations

EEFI- Essential elements of friendly information

ELINT- Electronic Intelligence

EW- Electronic Warfare

FIS- Foreign Intelligence Service

FOIA- Freedom of Information Act

FOUO- For Official Use Only

FPCON- Force Protection Condition

GCA- Government Contracting Activity

HUMINT-Human Intelligence

IMINT- Imagery Intelligence

IA- Information Assurance

INFOSEC- Information Security

IO- Information Operations

IOSS- Interagency OPSEC Support Staff (A division of the National Security Agency)

ITAR- International Traffic in Arms Regulations

MASINT- Measurement and Signatures intelligence

MILDEC- Military Deception

NIPRNet-Non-classified Internet Protocol (IP) Router Network

NISPOM- National Industrial Security Program Operating Manual (DoDINST 5220.22M) NNPI- Navy Nuclear Propulsion Information

NOFORN- Not Releasable to Foreign Nationals/Governments/Non-US Citizens

NOTAM- Notice to airmen (Also: Notice to Mariners)

OPSEC- Operations Security

OSINT- Open-source Intelligence

PAO- Public Affairs Office/Public Affairs Officer

PEO- Program Executive Officer

PII- Personally Identifiable Information (Privacy Act Information) PKI- Public Key Infrastructure

PMO- Program Management Office

POC- Point of Contact

PPP- Program Protection Plans

R&D- Research and Development

RDT&E- Research, Development, Test, and Evaluation

SAP- Special Access Program

SBIR- Small Business Innovative Research

SCG- Security Classification Guide

SCI- Sensitive Compartmented Information

SIGINT- Signals Intelligence

SIPRNet-Secure Internet Protocol (IP) Router Network

SOP- Standard Operating Procedure

SOW- Statement of Work

SWF- U.S. Army Corps of Engineers, Fort Worth District
TDY- Temporary Duty

TTP- Tactics, Techniques, and Procedures

WMD- Weapons of Mass Destruction

TERMS

Adversary- Individuals, organizations, or countries that must be denied critical information in order to preserve mission integrity and maintain friendly mission effectiveness and the element of surprise. Adversary, in this context, includes any individual, organization, or country with which specific information should not be shared to preserve mission integrity or the element of surprise.

Classified military information- Information originated by or for the DOD or its agencies or under their jurisdiction or control that requires protection in the interest of national security. It is designated TOP SECRET, SECRET, or CONFIDENTIAL as described in Executive Order 12958 or subsequent order. Classified military information may be in oral, visual, documentary, or materiel form.

Communications security (COMSEC)- Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications.

Competitive Intelligence- Describes the legal and ethical activity of systematically gathering, analyzing and managing information on industrial competitors. Competitive intelligence is an ethical and legal business practice, as opposed to industrial espionage which is illegal.

Computer security (COMPUSEC)- Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

Contractor- Refers collectively to the Contract Company and its personnel.

Controlled Unclassified Information (CUI)- Unclassified information to which access or distribution limitations have been applied according to national laws, policies, and regulations of the United States Government (U.S. Government). It includes U.S. information that is determined to be exempt from public disclosure according to DODD 5230.25, DODD 5400.7, and so on, or that is subject to export controls according to the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR). This includes FOR OFFICIAL USE ONLY, Unclassified-NNPI, and PII etc.

Counterintelligence (CI)- Those activities which are concerned with identifying and counteracting the threat to security posed by foreign intelligence services or organizations, or by individuals engaged in espionage, sabotage, subversion or terrorism.

Cover- Actions used to conceal actual friendly intentions, capabilities, operations and other activities by providing a plausible, yet erroneous, explanation of the observable.

Critical Information- 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. Critical information 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. Critical information is information that is vital to a mission that if an adversary obtains it, correctly analyzes it, and acts upon it will prevent or seriously degrade mission success. Critical information can be classified information or unclassified information. Critical information can also be an action that provides an indicator of value to an adversary and places a friendly activity or operation at risk. The term “critical information” has superseded the term “Essential Elements of Friendly Information” (EEFI). EEFI now refers to critical information phrased in the form of a question in order protect classified and sensitive information.

Critical Information List (CIL)- The CIL is a consolidated list of a unit or organization’s critical information. The CIL will be classified if any one of the items of critical information is classified. The method to ensure the widest dissemination of a unit or organization’s critical information is to convert it to Essential Elements of Friendly Information (EEFI). EEFI is critical information phrased in the form of a question that does not reveal the details of critical information in order to prevent disclosure of classified and sensitive information.

Critical Program Information (CPI)- Information, technologies, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction. This includes classified military information or controlled unclassified information (CUI) about such programs, technologies, or systems. CPI is a form of critical information specific to acquisition programs.

Electronic Security (ELSEC)- The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of non-communications electromagnetic radiations, for example, radar.

Essential Elements of Friendly Information (EEFI)- The EEFI is critical information phrased in the form of a question that does not reveal the details of critical information in order to prevent disclosure of classified and sensitive information. EEFI are phrased as questions that the adversary is likely to ask about friendly capabilities, activities, limitations, and intentions. The use of EEFI is an effective way to ensure the widest dissemination of a unit or organization’s critical information while protecting classified and sensitive information. “Critical information” supersedes the term “Essential Elements of Friendly Information” (EEFI). DOD and the Service Components are now using the term “critical information” for the purpose of standardization.

Essential Secrecy- The condition achieved from the denial of critical information to adversaries.

For Official Use Only (FOUO)- A designation that is applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA). (A form of CUI)

Force Protection- A security program consisting of actions taken to prevent or mitigate hostile actions against all DA personnel (Military personnel, DoD Civilians and DOD contractors, and family members), resources, facilities, and critical information. Force protection does not include actions to defeat the adversary or protect against accidents, weather, or disease.

Friendly- Individuals, groups or organizations involved in the specific operation or activity that has a need to know.

Government Contracting Agency (GCA)- A Government Contracting Agency is an element of a federal department or agency that is designated by the agency head and is delegated broad authority regarding acquisition functions.

Indicators- Data derived from open sources or from detectable actions that adversaries can piece together or interpret to reach personal conclusions or official estimates concerning friendly intentions, capabilities or activities.

Information Security (INFOSEC)- INFOSEC is the system of policies, procedures, and requirements established under the authority of Executive Order (EO)12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

Information Superiority- The degree of dominance in the information domain which permits the conduct of operations without effective opposition.

Intelligence- The product resulting from collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign areas, operations or activities.

Military Deception (MILDEC)- Actions executed to mislead foreign decision makers, causing them to derive and accept desired appreciations of military capabilities, intentions, operations or other activities that evoke foreign actions that contribute to the originator’s objectives.

Observables- Actions that convey indicators exploitable by adversaries but that must be carried out regardless, to plan, prepare for and execute activities. (e.g: Loading special equipment onto trucks or arrival of special shipments that can be “Observed” by our adversaries.)

Operations Security- Operations security (OPSEC) is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence systems;

b. Determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and

c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

OPSEC Compromise- The disclosure of critical information or sensitive information which has been identified by the Command and any higher headquarters that jeopardizes the unit's ability to execute its mission or to adequately protect its personnel and/or equipment.

OPSEC measures- Methods and means used to gain and maintain essential secrecy about critical information. The following categories
apply:

a. Action control. The objective is to eliminate indicators or the vulnerability of actions to exploitation by adversary intelligence systems. Select what actions to undertake; decide whether or not to execute actions and determine the "who," "when", "where" and "how" for actions necessary to accomplish tasks.

b. Countermeasures. The objective is to disrupt effective adversary information gathering or prevent their recognition of indicators when collected materials are processed. Use diversions, camouflage, concealment, jamming, threats, police powers and force against adversary information gathering and processing capabilities.

c. Counter-analysis. The objective is to prevent accurate interpretations of indicators during adversary analysis of collected materials. This is done by confusing the adversary analyst through deception techniques such as covers.

OPSEC planning guidance- Guidance that serves as the blueprint for OPSEC planning by functional elements throughout the organization. It defines the critical information that requires protection from adversary appreciations, taking into account friendly and adversary goals, estimated key adversary questions, probable adversary knowledge, desirable and harmful adversary appreciations and pertinent intelligence system threats. It also should outline tentative OPSEC measures to ensure essential secrecy. This is also forms the contents of an OPSEC estimate.

OPSEC vulnerability- A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision-making.

OSINT- Open Source Intelligence. 80-90% of intelligence collection efforts occur through open sources; internet, media, trade show, trade magazines, etc.

Publicly accessible web site- An DoD web site with access unrestricted by password or Public Key Infrastructure user authorization. “Public” refers to the at-large audience on the Internet; anyone who can access a web site through a browser.

Public Release- The approved release of coordinated, consistent, accurate, and authoritative information that meets appropriate security regulations and Army/DoD guidelines for the release of information to the public. Release of SWF technical information must be approved by SWF Project Officer, SWF Office of Counsel, SWF Public Affairs Officer and SWF OPSEC Offier. The SWF Public Affairs Officer is the point of contact for all Public Release material.

Security manager- A properly cleared individual having professional security credentials to serve as the manager for an activity.

Sensitive activities- Sensitive activities are special access or code word programs, critical research and development efforts, operational or intelligence activities, cover, special plans, special activities, sensitive support to non-Army agencies and/or activities excluded from normal staff review and oversight.

Sensitive information- Sensitive information is information requiring special protection from disclosure that could cause compromise or threat to our national security, a Navy organization, activity, family member, DoD civilian or DOD contractor. Sensitive information refers to unclassified information while sensitive compartmented information (SCI) refers to classified information. Examples which may be deemed sensitive include but are not limited to: personal information; structuring; manning; equipment; readiness; training; funding; sustaining; deploying; stationing; morale; vulnerabilities; capabilities; administration and personnel; planning; communications; intelligence, counterintelligence, and security; logistics; medical; casualties and acquisition plans.

Sensitive Compartmented Information (SCI)- Information or material requiring special controls for restricted handling within compartmented intelligence systems and for which compartmentalization is essential. SCI rules are established by the Director of Central Intelligence and are covered in DOD C–5105.21–M–1.

Social Engineering- The art of manipulating people into performing actions or divulging confidential or critical information through deception.

Social Media- Refers to the means of interactions among people in which they create, share, and exchange information and ideas in virtual communities and networks; Facebook, Twitter, LinkedIn, etc.

Special Access Program (SAP)- A sensitive activity, approved in writing by the Secretary of Defense. It imposes extraordinary security measures to control access and provide protection of extremely sensitive information in addition to the provisions of AR 380–5. The controls depend on the criticality of the program and the intelligence threat.

TrashINT- A form of Open Source intelligence, achieved by **o**btaining sensitive information by searching through trash and recycling containers that are publically accessible.

Threat- Capability of a potential adversary to limit or negate mission accomplishment or to neutralize or reduce the effectiveness of a current or projected organization or material item. Intelligence collection threat (efforts by adversary to gain information) For OPSEC purpose this refers to HUMINT, OSINT, IMINT, SIGNINT, MASINT capabilities.

Unclassified Information- Information that may be sensitive in nature, is not classified by nature. Unclassified information is NOT releasable to the public without public release authority of the information owner.

RESOURCES

Defense Security Service.

www.dss.mil: DSS administers the National Industrial Security Program (NISP) on behalf of the Department of Defense and 26 other federal agencies. There are approximately 13,500 contractor facilities that are cleared for access to classified information. The Defense Security Service has an online training program for DoD and DoD Contractors.

The Interagency OPSEC Support Staff

https://www.iad.gov/ioss/index.cfm The primary responsibility of the Interagency OPSEC Support Staff (IOSS) is to act as a consultant to other U.S. government departments or agencies by providing technical guidance and assistance that will result in self-sufficient OPSEC Programs for the protection of U.S operations. Members of the IOSS staff assess OPSEC programs, assist in OPSEC program development, conduct surveys, assessments and provide OPSEC training.

The National Counterintelligence Executive.

http://www.ncix.gov/ As the premier counterintelligence and security agency in the US Government, the Office of the National Counterintelligence Executive will provide effective leadership and support to the counterintelligence and security activities of the US Intelligence Community, the US Government, and US private sector entities who are at risk of intelligence collection or attack by foreign adversaries.

OPSEC Professionals Society

www.opsecsociety.org OPS members are comprised of United States government, military, corporate and private practice professionals and those of our nation’s allies who specialize in the field of OPSEC, Counterintelligence, and other related disciplines.

SWF PUBLIC ACCESS WEB SITE

http://www.swf.usace.army.mil/BusinessWithUs/Contracting.aspx This site contains AT Level I training for contractors, OPSEC Level I training for contractors, and iWatch training and print materials for contractors.

DISCLAIMER The appearance of external hyperlinks does not constitute endorsement by the United States Department of Defense, the United States Department of the Navy and NAVSEA of the linked Web sites, or the information, products or services contained therein.

OPSEC GUIDANCE FOR CONTRACTING OFFICER REPRESENTATIVES & TECHNICAL SPECIALISTS