



## DEPARTMENT OF THE ARMY

PROGRAM EXECUTIVE OFFICE  
GROUND COMBAT SYSTEMS  
6501 E. ELEVEN MILE ROAD  
WARREN, MICHIGAN 48397-5000

REPLY TO  
ATTENTION OF

SFAE-GCS-ACT

30 September 2013

### MEMORANDUM FOR RECORD

SUBJECT: Project Management Armored Brigade Combat Team (PM ABCT) Operations Security (OPSEC) Plan

#### 1. References:

- a. PEO GCS OPSEC Plan, 14 February 2013.
- b. AR 530-1, Operations Security (OPSEC), 19 April 2007.
- c. AR 381-12, Threat Awareness and Reporting Program, 4 October 2010.

#### 2. General. This OPSEC Plan is a supplement to the PEO GCS OPSEC Plan.

a. **Applicability.** This PM ABCT OPSEC Plan is applicable to all personnel (military, civilian, and contractor) working with the PM ABCT program. It outlines actions to ensure protection of Program Information from an adversary's observation and collection. This Plan is appropriately nested and not meant to replace or circumvent the PEO GCS OPSEC Program or Reference 1.a.. OPSEC compliments and reinforces other security program disciplines by eliminating, concealing, or reducing indicators that can compromise critical information. PM ABCT will implement the principles outlined in this OPSEC Plan in concert with the other security program disciplines.

b. **PM ABCT Mission.** Deliver, Sustain and Modernize Combat Power for the Army's Armored Brigade Combat Team. Army's Executive Agent for Life Cycle Management of the Abrams, Bradley, Paladin, M88, M113, Knight family of vehicles and the Armored Multi-Purpose Vehicle (AMPV) program. Our fleet management responsibilities include the design, development, production, fielding and sustainment of lethal, survivable, reliable and safe ground combat systems.

c. **Purpose.** The purpose of this OPSEC Plan is to control sensitive information and to protect operations and activities that, if exploited, could seriously degrade or defeat current or future plans and activities. To eliminate or mitigate the possibility of exploitation, it is imperative

SFAE-GCS-ACT

SUBJECT: Project Management Armored Brigade Combat Team (PM ABCT) Operations Security (OPSEC) Plan

that all personnel are knowledgeable of and apply these procedures during the conduct of their daily mission planning tasks and activities.

### 3. Responsibilities.

#### a. Project Manager (PM):

- (1) Implement an OPSEC program.
- (2) Approve an OPSEC Plan specific to the operation of the Project Management Office (PMO) as a supplement to the PEO OPSEC Plan.
- (3) Appoint an OPSEC Officer or Coordinator for the PMO who will perform the requirements of the OPSEC Officer appropriate for the PMO.
- (4) Ensure appropriate OPSEC measures are taken within the PMO to preserve essential secrecy.
- (5) Plan for and implement OPSEC before, during, and after operations or other activities, including research and development testing and evaluation (RDT&E) that affect the combat capability of the U.S. Army. OPSEC will be part of the PM's initial planning guidance.
- (6) Provide annual reminders of the importance of sound OPSEC practices. These reminders will include OPSEC news releases in publications, OPSEC information bulletins, and OPSEC awareness briefings.

#### b. OPSEC Officer:

- (1) Direct and implement the OPSEC program.
- (2) Plan for and implement OPSEC before, during, and after operations or other activities, including RDT&E that affect the combat capability of the U.S. Army.
- (3) Chair the PM ABCT-level OPSEC Working Group (OWG) to coordinate OPSEC actions across the PM ABCT on a consistent basis.
- (4) In conjunction with other staff officers, develop the PM ABCT Critical Information List (CIL) or Essential Elements of Friendly Information (EEFI).
- (5) Develop and recommend OPSEC measures to be implemented in PM ABCT.
- (6) Conduct OPSEC reviews of operational plans and reports to ensure adherence to OPSEC policies and procedures.
- (7) Conduct OPSEC self-assessment using the published OPSEC guidance to determine whether the PMO is implementing its own OPSEC policies and procedures. The OPSEC Officer

SFAE-GCS-ACT

SUBJECT: Project Management Armored Brigade Combat Team (PM ABCT) Operations Security (OPSEC) Plan

will submit a written assessment with results and recommendations to the assessed PM and PEO OPSEC Officer.

(8) Ensure that training exercises include realistic OPSEC considerations and that any evaluation of a training exercise includes an evaluation of OPSEC procedures. Further, ensure that pre-exercise briefings include OPSEC, incorporating the threat, CIL/EEFI, and OPSEC measures.

(9) Coordinate with the Public Affairs Officer (PAO) and Freedom of Information Act (FOIA) Officer to ensure an OPSEC review is conducted before the release of information concerning any programs or projects.

(10) Ensure OPSEC training is conducted in accordance with Reference 1.b. and this OPSEC Plan.

(11) Integrate intelligence, counterintelligence, force protection, and Information Operations (IO) into OPSEC planning and practice as appropriate.

(12) Monitor the OPSEC programs of subordinate organizations by reviewing OPSEC Plans, survey results, exercise evaluations, and Inspector General reports.

(13) Conduct an annual OPSEC assessment.

(14) Prepare for PM signature an annual (by Fiscal Year) OPSEC Program Status Report to be submitted to the PEO OPSEC Officer.

(15) Perform other duties and responsibilities as defined in Reference 1.b., Appendix H.

c. PEO Webmaster:

(1) Comply with Federal, Department of Defense (DoD), and Department of the Army (DA) website administration policies and implement content-approval procedures that include OPSEC and PAO reviews before updating or posting information on all websites.

(2) Conduct quarterly OPSEC reviews of all organizational websites.

(3) Coordinate directly with the OPSEC Officer for additional guidance as needed on any questionable website posting.

(4) Receive Social Media and Operations Security training course at Information Assurance Training Center and DISA's Social Network Course.

SFAE-GCS-ACT

SUBJECT: Project Management Armored Brigade Combat Team (PM ABCT) Operations Security (OPSEC) Plan

d. All personnel:

- (1) Implement OPSEC measures as determined by the PM.
- (2) Receive Operations Security Level I training to—
  - (a) Understand how OPSEC complements traditional security programs to maintain essential secrecy of U.S. military capabilities, intentions, and plans
  - (b) Learn how to apply OPSEC to their daily tasks
  - (c) Learn why OPSEC is important to the organization
  - (d) Understand how adversaries aggressively seek information on U.S. military capabilities, intentions, and plans
  - (e) Become knowledgeable of the local multidiscipline adversary intelligence threat
  - (f) Become knowledgeable of PM ABCT's CIL and how to protect it by applying OPSEC measures to prevent inadvertent disclosure.
- (3) Maintain need-to-know and telephone security.
- (4) Limit distribution.
- (5) Avoid talking about work in public locations.
- (6) Safeguard unclassified technical data (also known as Controlled Unclassified Information [CUI]).
- (7) Be familiar with this OPSEC Plan and where to obtain additional OPSEC guidance as needed.
- (8) Handle any attempt by unauthorized personnel to solicit sensitive or critical information per Reference 1.c.. Report all facts immediately to the nearest supporting counterintelligence office and inform the chain of command.

4. OPSEC Security Considerations. All personnel will consider OPSEC when preparing policies, procedures, and doctrine; designing systems; or prescribing logistic or administrative practices. The OPSEC process applies to all phases of an activity, function, or operation. The five fundamental steps in the OPSEC process are as follows:

SFAE-GCS-ACT

SUBJECT: Project Management Armored Brigade Combat Team (PM ABCT) Operations Security (OPSEC) Plan

a. Identification of CIL or EEFI. Critical information is information associated with PM ABCT operations and activities that, individually or in the aggregate, reveals details about capabilities and intentions of planned or ongoing program activities. If an adversary obtains this information, it could prevent or seriously degrade mission success. EEFI is simply CIL posed in the form of a question in case the CIL is classified. It is imperative to understand that an answer to an EEFI is critical information and will be protected at all times Appendix 1 is the PM ABCT CIL/EEFI.

b. Analysis of Threats. Adversaries may conduct collection of information concerning PM ABCT activities using various intelligence collection methods. When aggregated, this information can provide an accurate portrayal of friendly intentions or operations. The aim is to neutralize or manipulate the threat. Collection threats are described in the PEO GCS OPSEC Plan; however, for detailed information about specific intelligence threats, the four questions that must be answered in relationship with threat analysis are as follows:

(1) What critical information is already known by the adversary?

(2) What gaps exist in the adversary information base that prevents it from deriving critical information?

(3) What intelligence collection assets are available that will enable the adversary to exploit friendly actions?

(4) What are potential OPSEC vulnerabilities?

c. Analysis of Vulnerabilities. This step identifies tentative OPSEC measures required to maintain essential secrecy. The most desirable OPSEC measures combine the highest protection with the least effect on PM ABCT operational effectiveness. Appendix 2 is a list of potential PM ABCT vulnerabilities and OPSEC measures.

d. Assessment of Risk. Because implementation of OPSEC measures usually presents a risk to operational, logistic, or procedural effectiveness, the OPSEC Officer will analyze them prior to the implementation decision. The OPSEC Officer makes recommendations on each measure based on the following three questions:

(1) What is the risk to operational effectiveness if this OPSEC measure is implemented?

(2) What is the risk to operations and the command mission success if this OPSEC measure is not implemented?

(3) What risk will result if this OPSEC measure fails to be effective?

SFAE-GCS-ACT

SUBJECT: Project Management Armored Brigade Combat Team (PM ABCT) Operations Security (OPSEC) Plan

e. Application of Appropriate OPSEC Measures. The OPSEC Officer will select OPSEC measures based on the previous steps. OPSEC measures aid in the elimination of indicators or the vulnerability of actions to exploitation by an adversary. The OPSEC measures in Appendix 2 apply to all PM ABCT personnel, and all personnel will adhere to them at all times. The PM will approve each OPSEC measure based on the OPSEC Officer's recommendations and the answers to the questions in paragraph 4.d. OPSEC measures are methods and means used to gain and maintain essential secrecy about critical information. The following categories apply:

(1) 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.

(2) 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.

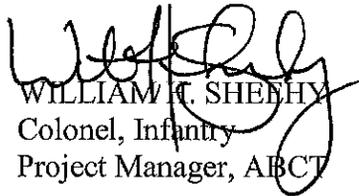
(3) Counter-analysis. The objective is to prevent accurate interpretations of indicators during adversary analysis of collected materials. Confuse the adversary analyst through deception techniques such as covers.

f. Conclusion. PM ABCT will continually monitor the OPSEC posture via OPSEC assessments and comparing personnel actions to the requirements of this OPSEC Plan. Additionally, the OPSEC Officer will remain abreast of the current threat situation by liaison with other intelligence and security elements in the PEO.

5. The point of contact for this OPSEC Plan is Larry Klann, commercial (586) 282-0330.

Encls

1. CIL/EEFI
2. Vulnerabilities and OPSEC Measures

  
WILLIAM C. SHEEHY  
Colonel, Infantry  
Project Manager, ABCT

## **Appendix 1: PM ABCT Critical Information List or Essential Elements of Friendly Information**

Critical information consists of specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment.

The Operations Security (OPSEC) Officer, in conjunction with a working group, develops the PM ABCT Critical Information List (CIL) or Essential Elements of Friendly Information (EEFI) for approval by the Project Manager. It is the PM's intent that all personnel (military, civilian, and contractors) are aware of this CIL so they can better apply OPSEC to their daily tasks.

The CIL/EEFI is as follows:

### **Critical Information:**

1. When, where and how often specific groups/teams/pairs of PM ABCT employees travel for government business, i.e., Intelligence Electronics Testing, Worldwide Armor Conference, C4ISR Conference, etc.
2. Specific and projected system vulnerabilities PM ABCT is working on enhancing vehicle survivability and sustainability. Be wary of announcing what specific areas on Survivability, Intelligence or Combat Improvements, Electronic Warfare, C4ISR, Mission Command upgrades.
3. Custom Computer software used in PM ABCT weapons system development, testing and evaluation. This includes Vetrionics, Fire Control, VICTORY, Wireless capabilities and limitations, Information Assurance and Crypto requirements. Each Systems Real Time Operating Environment and Computer language requirements.
4. Information Technology architecture and SharePoint portal system vulnerabilities.
5. Identification of Critical Program Information (CPI) and Program Protection Plan (PPP) Implementation methods - Location of CPI within the weapon system; identification of contractor Developing CPI; protection measures implemented to protect CPI and critical functions of the weapon system.
6. Operational readiness or specific equipment on a vehicle that is causing any operational issues of ABCT units deployed or being deployed. If in the future wireless downloading of vehicle data is authorized, download of a single vehicle's data will be FOUO but download of entire unit's data could identify a vulnerability or limitation for combat operations.
7. Photos of or information about vehicles or equipment that have been damaged by Threats. Combat damage photos of any vehicle should not be commented on, noted or discussed in open forum. No discussion of what type of IED Jammers or IED defeat systems being worked on. Any information or threat comments on anything that hits and penetrates our vehicles should not be posted on NIPR or open source.

SUBJECT: PM ABCT Operations Security (OPSEC) Plan

8. Specific friendly force technology areas of details, organizational initiatives, and Operational procedures designed to counter IEDs. This includes IED CONOPS, IED TTPs, IED Counter Devices, Counter IED Capabilities or Limitations, Ongoing Counter IED upgrades.
9. PM ABCT vehicle equipment, technological, organizational, or operational capabilities. This would also include future, projected or targeted capabilities.
10. Classification levels of the program - Special Compartmented Information (SCI) and Special Access Program (SAP) accesses; Security Classification Guide (SCG) identifies classified critical Information; Department of Defense (DD 254), if addressing SCI or SAP.

**OPSEC Indicators.** OPSEC indicators are data derived from openly available information or detectable activities that an adversary can piece together or interpret to reach conclusions or estimates concerning program intentions, capabilities, or activities. The success of OPSEC depends on knowledge of how we are viewed from an adversary's perspective. If necessary, we will modify our actions, which will in turn change the perspective of an adversary.

The following list of OPSEC indicators should not be considered all-inclusive.

- Budget data that provide insight into objectives and scope of the ABCT R&D.
- Solicitations for subcontractors to perform portions of the work.
- ABCT information on test and exercise schedules that allows adversaries to better plan tests and exercises through the use of their intelligence collection assets.
- ABCT testing conducted on the same location.
- List of ABCT personnel that handle classified information.
- ABCT equipment or system hardware itself.
- Unusual security clearance requirements.
- Use of words indicating irregular activity (e.g. Critical, Rush, Priority, Sensitive).
- Canceling leaves/recalling personnel to organization.
- Posting of schedules, orders, flight itineraries, organizational charts, etc.
- Discussing personnel, intelligence, operations, logistics, and plans over non-secure equipment.
- Unusual or increased levels of TDY and conferences by senior officials and staff members.
- Discussing problems or adverse personnel actions of individuals over non-secure equipment.
- Security clearances annotated on TDY orders.
- Conducting rehearsals for special activities.
- Coordination with personnel at different locations.
- Increased volume and priority of requisitions.
- Planning for ABCT conferences, symposia, and internal professional forums.
- ABCT package or container labels that show the name of an operation, program designation and the classification.

## Project Management Armored Brigade Combat Team (PM ABCT) Operations Security (OPSEC) Plan

### Appendix 2 – PM ABCT Vulnerabilities and OPSEC Measures

1. **Vulnerabilities.** Vulnerabilities exist when an adversary can collect OPSEC indicators of critical information, correctly analyze the information, decide on an action, and execute the action. Their goal is to either prevent mission accomplishment or adversely affect mission success.

The following vulnerabilities were derived by comparing the intelligence collection threat against the PM ABCT daily work routine.

a. Failure to use proper e-mail security when transmitting Controlled Unclassified Information (CUI) (FOUO, technical data, or Personal Identifiable Information (PII)) or critical information. CUI is susceptible to compromise when e-mailed without the proper security settings activated.

b. Information left unattended. Program information that is left in a conference room, vehicle, or hotel becomes susceptible to compromise or loss. Information that can be viewed, lost or compromised may provide an adversary with valuable data that would allow them to develop systems to defeat our efforts, vehicles or equipment. In the same respect, PII that is left in a conference room, vehicle or hotel can lead to an individual becoming the victim of identity theft. Examples of PII information that if left unattended could lead to identity theft are: banking information, identification cards, medical paperwork, and personal data that has your social security number.

c. Unauthorized disclosure of test schedules, locations, and purpose allow Foreign advocates to target our activities with HUMINT, IMINT, MASINT, and SIGINT resources. A lack of adequate OPSEC considerations during test planning and execution, to include movement of people and vehicles and site preparation could disclose test objectives, and other classified or unclassified program information.

d. Industry Day, Symposiums, Meetings, or Professional Conferences should all have OPSEC considerations. Personnel are susceptible to elicitation and exploitation of information when attending these events by fellow participants or personnel from foreign countries. Personnel may also inadvertently make themselves a target for intelligence agency with a point of contact for future information gathering attempts. Collection efforts may range from innocuous questions to actual blackmail by intelligence agents.

e. Conference Room or Defense Connect on Line (DCO) Security. Unauthorized or inadvertent release of PM ABCT information to non PM ABCT personnel supporting the effort. Organizations within PM ABCT currently operate in a competitive environment and all material should be handled appropriately and protected at the classification level assigned. The host of all DCO meetings and the U.S. Government participants need to be diligent in ensuring that our contractor's completion of sensitive FOUO information is not compromised. The DCO Host will not allow individuals logging in as "guest." Users must log in as registered users. This will stop guest entering fake names as their log-in and will ensure that users logging in at all times have a need to know.

f. Failure to properly protect OPSEC considerations for meetings and briefings. Example: "This brief is FOUO, No Contractors or Foreign participants can be present unless approved prior, and the Distribution Markings of the material being presented or provided. PM ABCT

SUBJECT: PM ABCT Operations Security (OPSEC) Plan

CUI information (via the internet, media, meetings, etc.) that has not gone through the public release process is not authorized for public release. Information that is released without authorization may provide valuable information regarding PM ABCT equipment and platform capabilities, vulnerabilities, limitations, and requirements. Such information would allow an adversary to develop systems to defeat our equipment in development.

g. Lack of OPSEC awareness. PM ABCT personnel do not fully realize their OPSEC responsibility in the protection of PM ABCT information. Personnel are not fully aware of the intelligence value of unclassified information and the adversary's capability to decipher important intelligence data from seemingly non-critical information.

h. Non-ABCT visitor within the facility may observe or hear program information, operations, or activities.

i. Communications/Transmissions: All unsecured telephone conversations (including cellular phones) are vulnerable to monitoring, and all long distance microwave transmissions are subject to intercept. Such vulnerabilities provide a source of information for intelligence agents. Communications supporting computer systems and faxes are equally vulnerable. Mailing program information is susceptible to interception or loss.

j. Teleconference and passcodes: Some PM ABCT subordinate organizations are currently operating in a competitive environment; therefore all information will be handled in a secure way. Teleconferences are an excellent way to share information, but we must ensure the communication process is done properly. The information discussed in teleconferences should be on a need to know basis and protected by all participating users. Facilitators, in order to keep the information secured do not share passcodes or passwords. Also, change passwords at least every six months. All teleconference participants must be registered users, guest users will not be allowed access to safe guard information.

SUBJECT: PM ABCT Operations Security (OPSEC) Plan

2. **OPSEC Measures.** OPSEC measures are methods and means used to gain and maintain essential secrecy relative to the PM's critical information. The most desirable OPSEC measures provide needed protection with the least amount of cost and impact on mission effectiveness and efficiency.

All personnel should know and employ the following OPSEC measures during their daily work routines. Application of these measures will prevent or mitigate the possibility of compromising critical information. The OPSEC Officer will develop additional OPSEC measures for crisis activities or as required.

a. All e-mails containing CUI, FOUO, PII or critical information will be encrypted or posted on the PM ABCT Knowledge Center, PM ABCT Information Data Environment or AKO.

b. When PII or PM ABCT information is not in use, it must be secured and out of plain view.

c. When testing is involved within the ABCT, OPSEC considerations need to be part of the testing process. An approved OPSEC briefing must be given prior to the test being conducted to all authorized personnel participating in the testing.

d. When participating in Industry Day, Symposiums, Meetings, or Professional Conferences, constant OPSEC awareness of potential threat and environment must be considered. Make sure that the facility is cleared (SECRET, Controlled Unclassified Information or Unclassified) for discussions or cleared to handle the information presented. Do not leave CUI or FOUO information unattended. When no longer needed, CUI, FOUO information must be shredded, to make unreadable or turned in to the security support staff for proper destruction. Make sure that you wear your ID badge only during the event. Secure badge from view when leaving the event. Report lost, or stolen badges immediately to the security support staff. Restrict ABCT conversations to designated areas (i.e. conference rooms), report any suspicious activity or contacts to Army Military Intelligence, if activity is off DoD installations contact the local police, FBI, 902<sup>nd</sup> or G2, TACOM LCMC.

e. In addition to security training, employees are also provided OCONUS Travel Training. This training is administered prior to the employee's travel to or through foreign countries. If available, receive an OPSEC threat briefing from G2, TACOM LCMC or the local Army Military Intelligence servicing that particular region prior to the activity.

f. Ensure that only authorized personnel associated with the program that have a need to know are only in attendance during a conference or when using DCO. Non PM ABCT personnel (i.e. SETA contractors not supporting PM ABCT, hotel/conference center staff, other government employees that do not have a need to know, etc.) will not be present in the room or dialed in during the conference session(s). Room set up and catering service will be done prior to the conference start or during breaks. While the conference is in session, all doors will remain closed and entry into the room monitored. Attendees will refrain from using cell phone while the conference is in session. Laptops and handout materials will be secured from unauthorized viewing during or while not in session.

g. PM ABCT information (documents, presentations, photos, videos, etc.) that is intended to be presented outside the PEO GCS, PM ABCT and the DoD must be submitted and approved for

SUBJECT: PM ABCT Operations Security (OPSEC) Plan

public release. The public release process will consist of an OPSEC Review and technical review of the information to be presented to the general public to ensure that the information is current and accurate. Release of information outside PEO GCS, PM ABCT or DoD must be submitted for OPSEC review and to validate the receiving entity can protect the information commensurate with DoD, PEO GCS and PM ABCT protection measures. Information that is CUI will not be approved for public release.

h. Increase OPSEC awareness through initial and annual OPSEC training, providing periodic OPSEC reminders through e-mails/newsletters, posting and periodically rotating OPSEC posters in work areas. A copy of the OPSEC plan will be made available for information and reviews. Conduct OPSEC site survey visits to various PM ABCT locations.

i. Visitors to PM ABCT facilities are required to process through established checkpoints for verification of identity, citizenship, personnel security clearances, appropriate certification of purpose of visit, and inspection of articles being brought into and out of the facility, before classified or unclassified information will be released. Visitors to PM ABCT facilities or areas will be escorted at all times. Escorts for visitors shall be advised of proper escort procedures, limitations on disclosure, and other applicable controls involved in the visit. Personnel within the area should be made aware of the visitor and reminded to secure CUI information from visitor view. Personnel should also be mindful of the visitor's presence during telephone conversations. Be aware of custodial and maintenance personnel within the area. Foreign national visitors may not access areas before the security representative and export focal have been informed. Prior to a foreign national visit, an e-mail will be sent to all personnel notifying them of the pending visit and to implement appropriate OPSEC procedures for the protection of PM ABCT information. In some cases foreign visitors may be in a different part of the building but share common areas with program personnel. OPSEC procedures should be implemented so program information is not discussed in open areas. Foreign visitors are limited to the restrictions identified on the foreign visit request and must be escorted by a trained escort at all times.

j. All new PM ABCT personnel will be trained on Security Procedures during the quarterly new ABCT personnel meeting. Security education will include awareness among ABCT personnel concerning the use of communications devices. Discussions of a classified nature via unsecured telephone are absolutely prohibited. For CUI data exchanges outside DoD networks, use only NIST/NIAP compliant solutions. Landline communications for telephone conversations are more secure than cellular and should be utilized whenever available for DoD, PEO GCS or PM ABCT CUI discussions. All printed media and faxes will be retrieved immediately.



**Program Executive Office  
Ground Combat Systems (PEO GCS)  
Operations Security (OPSEC) Plan**

**14 March 2013**

PREPARED BY: Security Office, PEO GCS, SFAE-GCS-CIO/ms 505, 6501 East Eleven  
Mile Road, Warren, MI 48397-5000

**OPERATIONS SECURITY (OPSEC) PLAN  
VERSION 1.0**

**14 MARCH 2013**

\*\*\*\*\*

SUBMITTED BY

E-Signed by CHAPLIN, NANCY, A.1230490259  
VERIFY authenticity with ApproveIt   
**CHAPLIN.NANCY.A.1230490259**

-----  
NANCY CHAPLIN  
Senior Security Officer

APPROVAL

E-Signed by DAVIS, SCOTT, JEFFREY, 1095741122  
VERIFY authenticity with ApproveIt   
**DAVIS.SCOTT.JEFFREY.1095741122**

-----  
SCOTT J. DAVIS  
Program Executive Officer,  
Ground Combat Systems

# Change History

OPSEC Plan Control Information						
<b>Document ID:</b>	<b>Document Owner:</b>	<b>Document Approver:</b>	<b>Date Effective:</b>	<b>Version:</b>	<b>Retention Period:</b>	<b>Archive Location:</b>
GCS_OPSEC_Plan	Security Officer	PEO	20130314	1.0	Review Annual	PEO GCS Portal

The following Change History log contains a record of changes made to this document:

Published / Revised Date	Version #	Author (optional)	Section / Nature of Change
03/14/2013	1.0	Chaplin, Nancy	Initial

# Table of Contents

<b>PEO GCS Mission Statement .....</b>	<b>1</b>
<b>Assignment of OPSEC Responsibilities .....</b>	<b>1</b>
OPSEC Definition .....	2
OPSEC Concept .....	2
OPSEC Compromise .....	4
Penalties.....	4
Limits on Secrecy .....	4
Individual Responsibilities .....	5
Program Executive Officer (PEO) .....	5
Senior Security Officer .....	5
OPSEC Officer .....	5
Public Affairs Officer (PAO) .....	6
PEO Webmaster .....	7
Project Managers (PM) .....	7
Assistant Program Executive Officers.....	8
All personnel .....	8
<b>OPSEC Considerations.....</b>	<b>8</b>
<b>Critical Information.....</b>	<b>9</b>
<b>OPSEC Measures.....</b>	<b>10</b>
OPSEC Awareness.....	11
Administrative/Personnel .....	11
Waste Disposal .....	12
Conferences/Symposia .....	12
Conference Room Security.....	12
Unsolicited Requests for Information .....	13
Compromising Emanations .....	14
Communications Security .....	14
Computer Security .....	15
Employee Travel .....	16
Shipment of Sensitive Materials.....	16
Public Release .....	16
Web site OPSEC Reviews.....	16
Employee Disaffection .....	17
Document Markings .....	17
Protection Measures for CUI.....	18
Visitor Control.....	18
Escorts for Foreign Visitors .....	19
Contractor and Subcontract Requirements.....	19
<b>Annex A – The Intelligence Collection Threat .....</b>	<b>1</b>
Foreign Intelligence Service Threat .....	1
Terrorist Threat .....	1
Insider Threat .....	1
Criminal Threat (Outsider).....	1
Environmental Threat.....	2

Military Threat .....	2
Human Intelligence (HUMINT) .....	2
Signals Intelligence (SIGINT).....	3
Measurement and Signatures Intelligence (MASINT) .....	4
Imagery Intelligence (IMINT).....	5
Open Source Intelligence (OSINT) .....	6
Computer Intrusion for Collection Operations.....	6
Terrorism .....	7
Technology Transfer .....	7
Professional Conferences/Symposiums .....	8
Personnel Disaffection .....	8
<b>Annex B – Vulnerability Assessment .....</b>	<b>1</b>
Information Security Vulnerabilities .....	1
Operations Security Vulnerabilities .....	1
Physical Security Vulnerabilities .....	2
Information System (IS) Vulnerabilities .....	2
<b>Annex C – PEO OPSEC Program Matrix .....</b>	<b>1</b>
<b>Annex D – OPSEC Checklist .....</b>	<b>1</b>
<b>Annex E – Terms.....</b>	<b>1</b>
<b>Annex F – References .....</b>	<b>1</b>

## **PEO GCS Mission Statement**

Execute life cycle management of the world's best ground combat systems in a collaborative learning environment by developing, acquiring, and supporting modernized and affordable systems with common integrated capabilities, always focusing on the needs of the Joint Warfighter.

## **Assignment of OPSEC Responsibilities**

This publication specifically addresses the common features of a functional, active and documented Operations Security (OPSEC) program. This publication assigns OPSEC responsibilities and requirements within the Program Executive Office, Ground Combat Systems (PEO GCS) to plan for and implement OPSEC; a systematic approach to developing necessary OPSEC measures; implementation of OPSEC training; requirements for the review of OPSEC measures and reporting; and cross-command and interagency support to the PEO GCS OPSEC program, which includes reviews, assessments, and survey training. It is designed to provide a basic understanding of OPSEC functions and how to apply them within PEO GCS. Each Project Management Office (PMO) of the PEO may require a unique approach to OPSEC depending on the PMO function. Each PMO will write an OPSEC Plan to address considerations not addressed in this PEO Plan. The basic concepts set forth herein are essentially the same for every organizational element of the PEO. OPSEC is applicable to all aspects of work, from daily routine planning through testing, exercise, and evaluation phases to force deployment, recovery, and reconstitution.

PEO OPSEC Officer: Nancy Chaplin, 586-282-9648

This OPSEC Plan documents the policies and procedures needed to meet the specific OPSEC program requirements of PEO GCS and to support the OPSEC programs of higher echelons.

The overall purpose of OPSEC is to strengthen our traditional security procedures by identifying existing vulnerabilities or weaknesses and applying measures to protect sensitive technologies. The goal is to deny our adversaries access to any critical information. Critical information includes technologies and information desired by an adversary that is sensitive and the disclosure of which could seriously impact our programs. Technology or information does not have to be classified to be of value to an adversary. An adversary can learn a lot about our programs by piecing together obtainable unclassified information. Therefore, in our attempts to shield our activities, it is not only important to follow normal security practices but also to implement OPSEC measures. This OPSEC Plan will discuss the five-step process:

1. Identifying Critical Information
2. Analysis of Threats

3. Analysis of Vulnerabilities
4. Assessment of Risks
5. Application of OPSEC Measures.

OPSEC applies to all organizations within PEO GCS. All information identified as critical information will be reviewed for OPSEC before being released to Government agencies outside PEO GCS. All information, regardless of whether it is critical, will be reviewed for OPSEC before its release to the public in any manner.

## **OPSEC Definition**

OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to—

1. Identify actions that can be observed by adversary intelligence systems.
2. Determine indicators that hostile intelligence systems can obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.
3. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

## **OPSEC Concept**

Many activities normal to daily functioning will convey information and indicators to adversaries in spite of routine security measures (personnel, physical, document, cryptographic, computer) to protect classified information. Information available from detectable friendly activities, when combined with other information held by an adversary will, in unknown ways, shape the adversary's appreciations and perceptions of friendly intentions, military capabilities, actions, and possible weaknesses, all of which will provide answers to adversary intelligence questions. During classified or sensitive unclassified undertakings (e.g., operations, exercises, field tests of military systems), acting routinely can result in adversaries gaining harmful appreciations by piecing together observable critical indicators.

Intelligence systems function worldwide. Even if PEO GCS is vigilant, other organizations that provide support may conduct activities that convey pertinent PEO GCS information or indicators of intentions, capabilities, limitations, and vulnerabilities. Therefore, planning for primary and supporting operations and other activities (e.g., a test administered by the Army Test and Evaluation Command [ATEC]) must include systematic examination to determine potential disclosures that would cause cancellation or failure of the primary undertaking. Subsequently, one must plan and execute protective measures that permit operations and activities to proceed effectively while preserving requisite essential secrecy. OPSEC is the process designed to do this.

An OPSEC vulnerability exists when an adversary can collect indicators of critical information, process the information, and react in a way harmful to the United States. The most serious problem facing PEO GCS in this respect is that critical information collected by an adversary today may allow the adversary to develop a technological advantage in the future. Collection capabilities used to obtain information from accessible activities generally depend on some form of target cooperation. For example, throwing any information in the trash allows it to be retrieved by an adversary who will gain information about our activities, and releasing information into the public domain allows the adversary to obtain useable information at no risk to their assets. The detection of predictable actions depends on our acting in stereotyped ways. Thus, if proper OPSEC measures are applied, it is often possible to eliminate or control many detectable indicators of critical information about our intentions, capabilities, limitations, and activities. Remember; trash cans are for non-informational items only (e.g., food waste, wrappers). All unclassified informational material will be placed in the secure shred boxes located throughout PEO GCS facilities.

The key objective of OPSEC is to ensure mission effectiveness. Some protective measures to eliminate information conveyed by an activity may unacceptably reduce effectiveness. For example, telemetry and communications are often needed in tests; and personnel, equipment, and material movements are unavoidable in the execution of operations and other activities. In these instances, it may be possible to deny information by acting against the collectors or analysts, rather than stopping the actions. Denial actions include the use of jamming, obscurants, weather, camouflage, environmental conditions, covers, or military deception (MD) to influence adversary perceptions and conclusions (e.g., cover operations to explain observable activities, diversions to draw collection and analytical interest elsewhere, creating conditioning to cause activities to be ignored, multiple impressions to confuse interpretation of information). In Joint operations, OPSEC is an element of command and control warfare (C2W). Countering the adversary command and control (C2), and protecting friendly C2 are functions of OPSEC.

Planning for secrecy must extend beyond exposure of raw information and consider possible assumptions and estimates made by an adversary. Logical conclusions based on generally available information, trend analysis based on historical data or technical possibilities, and broad experience of adversary planners and decision makers must be factored in to planning. Military deception may be required to mislead adversary analysts to maintain essential secrecy.

The following are examples of unclassified information that could alert an adversary to the existence of a classified project, existence or application of advanced technology, or a new tactic or technique unknown to adversaries:

- Unclassified agreements between government agencies or their association in a project or operation that outlines methods, procedures, and current U.S. Government intentions or future objectives.
- Special or unique requests providing special instructions that could reveal capabilities or the technology of a new weapon system.

- Public relations release describing aspects of technological or operational cooperation between the U.S. and other nations.
- Announcements of formation of specialized groups, special elements, or organizations, which could signal special intentions, activities, or capabilities.
- Consolidated budget execution for specific projects, testing of items or tactics, and monies spent that are intended for future acquisition.

## OPSEC Compromise

An OPSEC compromise is the disclosure of critical or sensitive information that jeopardizes PEO GCS's ability to execute its mission or to adequately protect its personnel or equipment. Good OPSEC practices can prevent these compromises and allow us to maintain essential secrecy about our operations.

Critical or sensitive information that has been compromised and is available in open sources and the public domain should not be highlighted or referenced publicly outside of intragovernmental or authorized official communications, because these actions provide further unnecessary exposure of the compromised information. Report any known or suspected OPSEC compromise to the PEO Security Office immediately.

## Penalties

Failure to comply with these orders, directives, or policies may be punished as violations of a lawful order under Article 92 of the [Uniform Code of Military Justice](#) (UCMJ) or under other disciplinary, administrative, or other actions as applicable. Personnel not subject to the UCMJ who fail to protect critical and sensitive information from unauthorized disclosure may be subject to administrative, disciplinary, contractual, or criminal action.

## Limits on Secrecy

Take care in determining the required degree of secrecy for undertakings. Too much secrecy can harm effectiveness; too little can result in mission or system failure. Broad factors to consider include the following:

- Adversaries must have some knowledge of friendly capabilities and intentions so they will perceive threats.
- The public must have some knowledge of military capabilities to foster recruitment of required personnel, gain internal political support, ensure understanding of defense budgeting requests, and support defense alliances.
- The U.S. must rigorously test systems, procedures, doctrine, and tactics in realistic environments.
- Planners must thoroughly understand activities to realize optimal coordination and effectiveness of their undertakings.

## Individual Responsibilities

Every individual is ultimately responsible for the security of the information to which he or she has access. Each piece of information that an adversary can get access to fills in one more piece of the puzzle as it relates to our overall plan of action.

### Program Executive Officer

- Issue orders, directives, and policies to protect PEO GCS critical and sensitive information to clearly define the specific OPSEC measures that all PEO personnel should practice.
- Ensure that the OPSEC program and OPSEC measures are coordinated and synchronized with security programs, e.g., information security (INFOSEC), information assurance (IA), physical security, and force protection.
- Ensure that all official information released to the public, to include information released on the World Wide Web, receives an OPSEC review prior to dissemination.
- Establish a documented OPSEC program that includes as a minimum, OPSEC Officer appointment orders and an OPSEC Plan.
- Appoint an OPSEC officer in writing with responsibility for supervising the execution of proper OPSEC within the organization.
- Ensure that the appointed OPSEC Officer is of appropriate grade or rank, and receives appropriate training in accordance with (IAW) [Army Regulation \(AR\) 530-1](#), Operations Security (OPSEC), 19 April 2007.
- Approve the PEO GCS Critical Information List (CIL) and circulate it to all subordinates as widely as security permits.
- Provide guidance and direction to ensure that each subordinate organization understands, adapts, and applies the CIL to its mission and provides feedback.
- Weigh the risk in the mission against the costs of protection and decide what OPSEC measures to implement; and publish such measures in the OPSEC Plan.

### Senior Security Officer

- Serve as the principal staff officer for overall management of the security and OPSEC program. The Senior Security Officer is the proponent for OPSEC, but the entire organization will integrate OPSEC into planning and execution of the organization's activities.
- Ensure the integration and synchronization of the OPSEC program with the OPSEC program of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)).

### OPSEC Officer

- Direct and implement the OPSEC program.

- Plan for and implement OPSEC before, during, and after operations and other activities, including RDT&E that affect the combat capability of the Army; ensure that OPSEC is part of the PEO's initial planning guidance.
- Chair the PEO-level OPSEC Working Group (OWG) to coordinate OPSEC actions across PEO GCS on a consistent basis.
- Develop the PEO's CIL in conjunction with other staff officers.
- Develop and recommend OPSEC measures to be implemented within PEO GCS.
- Conduct OPSEC reviews of operational plans and reports to ensure adherence to OPSEC policies and procedures.
- Conduct OPSEC assessments, in writing, of PMOs using the published OPSEC guidance to determine whether the PMO is implementing PEO-directed and their own OPSEC policies and procedures; recommend corrective actions as necessary.
- Ensure that training exercises include realistic OPSEC considerations and that evaluation of training exercises includes evaluation of OPSEC procedures. Further, ensure that pre-exercise OPSEC briefings incorporate the threat, CIL, and OPSEC measures.
- Coordinate with the Public Affairs and Freedom of Information Act (FOIA) Officers to ensure that information concerning PEO GCS programs and projects is reviewed for OPSEC before being released.
- Ensure that all OPSEC training is IAW AR 530-1 and this OPSEC Plan.
- Integrate intelligence, counterintelligence, force protection, and Information Operations (IO) into OPSEC planning and practice.
- Monitor the OPSEC programs of subordinate organizations by reviewing OPSEC Plans, survey results, exercise evaluations, and Inspector General reports.
- Conduct an annual OPSEC assessment.
- Prepare for the PEO's signature the annual (by Fiscal Year) OPSEC Program Status Report to be submitted to the Army OPSEC Support Element (OSE).
- Perform other duties and responsibilities as defined in AR 530-1, Appendix H.

### **Public Affairs Officer**

- Comply with Federal, Department of Defense (DoD), and Department of the Army (DA) website administration policies and implementing content-approval procedures that include OPSEC.
- Consider OPSEC in preparation of all public releases of official information.
- Coordinate with the OPSEC Officer before updating or posting information on all Web sites, IAW [AR 25-2](#), Information Assurance, Rapid Action Revision (RAR) 001, 23 March 2009, paragraph 4-20.g.(11).
- Ensure that in addition to the OPSEC Officer, the webmaster and other appropriate designees (e.g., command counsel, force protection, intelligence) have properly cleared information prior to posting to the web, unclassified intranet, or to Army Knowledge Online (AKO) areas accessible to all account types.

- Coordinate directly with the OPSEC Officer on all questionable releases and for additional guidance on any release, IAW [AR 530-1](#), paragraph 2-3.a.(15).
- Ensure that all military, civilian, or contractor personnel who post or maintain information (e.g., documents, spreadsheets) in the public domain for official PEO GCS purposes (also including OPSEC Officers and PAO personnel) complete “Social Media and Operations Security” training at [Information Assurance Training Center](#) or [DISA’s Social Network Course](#); or such similar courses that may be required in the future
- Ensure that all PEO personnel are aware of and support the OPSEC program, including OPSEC reviews IAW [AR 530-1](#).
- Consider OPSEC in all public affairs planning and execution procedures in support of antiterrorism (AT) efforts IAW [AR 525-13](#), Antiterrorism, 11 September 2008, Appendix D.
- Provide unclassified information about the Army and its activities to the public with maximum disclosure and minimum delay. Do not release information that would adversely affect national security, threaten the personal safety, or invade the privacy of members of the Armed Forces, IAW [AR 360-1](#), The Army Public Affairs Program, 25 May 2011, paragraph 2-3.d.(5).

### **Webmaster**

- Comply with Federal, DoD, and DA website administration policies and implement content-approval procedures that include OPSEC and PAO reviews before updating or posting information on all websites IAW [AR 25-2](#), paragraph 4-20.g.(11).
- Conduct annual OPSEC reviews of all organizational websites and provide these results to the OPSEC Officer for inclusion in the annual OPSEC report IAW [AR 25-2](#), paragraph 4-20.g. (15).
- Coordinate directly with the OPSEC Officer for additional guidance on any questionable website posting.
- Take the Social Media and Operations Security training course at [Information Assurance Training Center](#) or [DISA’s Social Network Course](#).

### **Program Managers**

- Implement an OPSEC program.
- Approve an OPSEC Plan specific to the operation of the PMO as a supplement to the PEO GCS OPSEC Plan.
- Appoint an OPSEC Officer or Coordinator to perform those requirements of the OPSEC Officer that are appropriate for the PMO.
- Ensure appropriate OPSEC measures are taken within the PMO to preserve essential secrecy.
- Plan for and implement OPSEC before, during, and after operations and other activities, including RDT&E that affect the combat capability of the Army; ensure that OPSEC is part of the PM’s initial planning guidance.

- Provide annual reminders of the importance of sound OPSEC practices, including but not limited to OPSEC news releases in publications, OPSEC information bulletins, and OPSEC awareness briefings.

### **Assistant Program Executive Officers**

- Ensure appropriate OPSEC measures are taken within the staff or section to provide maximum protection of all functions and activities.
- Assist the OPSEC Officer with integrating OPSEC into all organizational activities.

### **All Personnel**

- Implement OPSEC measures as determined by the PEO.
- Receive Operations Security Level I training IAW [AR 530-1](#), Chapter 4, to—
  - Understand how OPSEC complements traditional security programs to maintain essential secrecy of U.S. military capabilities, intentions, and plans.
  - Learn how to apply OPSEC to daily tasks.
  - Learn why OPSEC is important to the organization.
  - Understand how adversaries aggressively seek information on U.S. military capabilities, intentions, and plans.
  - Become knowledgeable of the local multidiscipline adversary intelligence threat.
  - Become knowledgeable of PEO GCS critical information and how to protect it by applying OPSEC measures to prevent inadvertent disclosure.
- Maintain need-to-know and telephone security.
- Limit distribution.
- Avoid talking about work in public locations.
- Safeguard unclassified technical data (also known as Controlled Unclassified Information [CUI]).
- Be familiar with this OPSEC Plan and where to obtain additional OPSEC guidance if needed.
- Handle any attempt by unauthorized personnel to solicit sensitive or critical information as an incident per [AR 381-12](#), Threat Awareness and Reporting Program, 4 October 2010. Report all such incidents immediately to the nearest supporting counterintelligence office and inform the chain of command.

## **OPSEC Considerations**

All personnel will consider OPSEC when preparing policies, procedures, and doctrine; when designing systems; and when prescribing logistic and administrative practices.

Policies, procedures, and doctrines govern the freedom of action and can introduce a degree of rigidity in the way functions are performed. Over time, the constraints imposed and procedural habits will become apparent, allowing adversaries to better

predict what organizations will or will not do and how the organization carries out various functions.

Systems and tactics are of little value if an adversary develops the capability to locate, track, identify, target, and destroy the system or counter the tactic when it is deployed or implemented. Administrative and logistic practices are generally overt and can reveal information of considerable value to an adversary. Standard ways of executing tasks make it simple to detect changes in routines, or against a specific background, to detect capabilities being readied for use.

## Critical Information

Critical information consists of specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment.

The OPSEC Officer, in conjunction with a working group, develops the PEO GCS overall CIL, which is then approved by the PEO. The PEO's intent is that all personnel—military, civilian, and contractors—are aware of the organization's critical information so they can better apply OPSEC to their daily tasks.

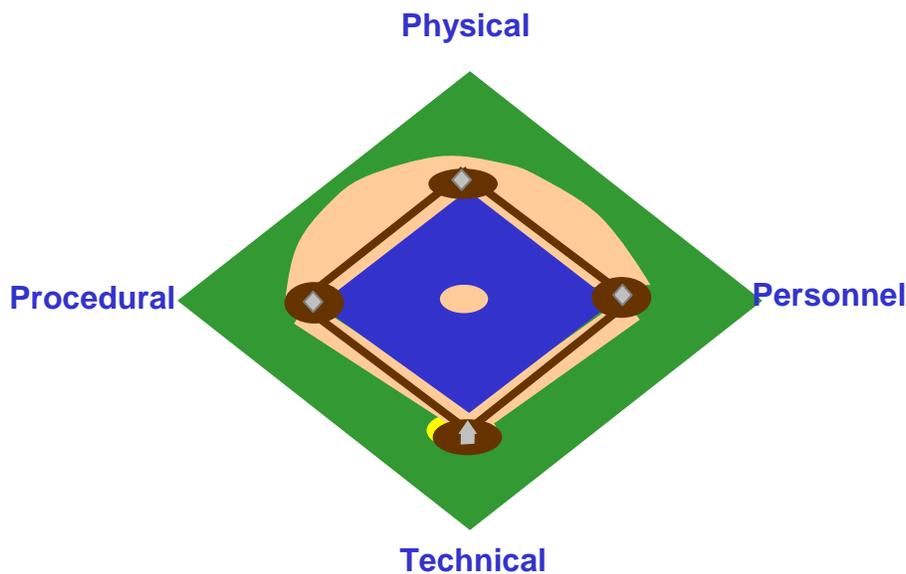
The overall PEO CIL is as follows:

- **Vulnerabilities and limitations in weapons and weapons systems** – Operational limitations (weather, terrain); reliability or effectiveness of the weapon system; lack of performance or identification of damage against threat (e.g., ballistic, non-ballistic, nuclear, chemical, biological, electronic warfare)
- **Weapons systems development schedules below summary** – Specific date, time, or location information prior to and during the event
- **Emerging technologies applicable to new weapons systems**
- **Custom computer software used in weapons systems development, testing and evaluation**
- **Identification of Critical Program Information (CPI) and Program Protection Plan (PPP) implementation methods** – Location of CPI within the weapon system; identification of contractor developing CPI; protection measures implemented to protect CPI and critical functions of the weapon system
- **Specifics or requirements of the program in acquisition** – Threshold and Objective specifications and technical performance measures
- **Preliminary programmatic and resourcing decisions not yet approved by the Army** – Program or contract cancellations; pre-Program Objective Memorandum (POM) or Budget Estimate Submission (BES) lock budget data; shortfalls in meeting program cost, schedule, and performance thresholds
- **Classification levels of the program** – Special Compartmented Information (SCI) and Special Access Program (SAP) accesses; Security Classification Guide (SCG) identifies classified critical information; Department of Defense (DD) Form 254, if addressing SCI or SAP

# OPSEC Measures

OPSEC measures are in place to protect identified critical information. A good way to evaluate an OPSEC measure is to start by considering its primary intended purpose and then consider any ancillary functions it performs. Since many OPSEC measures rely on their combination with other types of security functions it is helpful to "round the bases" of the security diamond to determine all aspects of the OPSEC measure. Possible OPSEC measures are as varied as the specific vulnerabilities they address.

## OPSEC Measure Types



**Example:** Access control devices are physical security devices, but they rely on personal security procedures to dictate who should be allowed entry and who should be denied. Access control devices also rely on employee compliance with procedures to walk through such devices and to identify themselves by badge, ID number, or biometric measurements. If the employees do not uniformly comply with these procedures, the device is not effective. If an analyst accepts that access control hardware is effective by its very presence, he or she will have missed the true vulnerabilities in its effectiveness.

Information can be compromised in a variety of ways. Security education emphasizes the threat of overt and clandestine intelligence collectors. Conversations at work and off the job must not pertain to subjects that listeners do not have a need to know about. Information security is of vital importance to the PEO GCS OPSEC program. Security procedures (e.g., using only approved storage containers, double-checking offices before departure, having a clean desk policy, ensuring the need to know) protect classified and sensitive program related information.

OPSEC Officers and Coordinators will look at the total operations and activities and determine where in these operations and activities indicators of critical information are or can be collected by an adversary collection capability. After this determination, OPSEC Officers and Coordinators will determine the type of OPSEC measure that will counter or mitigate the adversary's collection efforts. The actual measure or measures, in most cases, will be normal security or protective actions conducted by various security disciplines. By using the OPSEC process, described in [AR 530-1](#), OPSEC Officers will determine who, what, when, where, why, and how to apply various measures. OPSEC officers will look at the total activity, as the adversary looks at the activity.

The measures identified here are not all-inclusive of those practiced in PEO GCS. OPSEC measures in this section apply to all personnel at all operating locations. The OPSEC measures outlined in this section are designed to eliminate, reduce, or counter the possible vulnerabilities identified earlier in this plan. PMs will develop supplements to this Plan that address appropriate OPSEC measures, including those relevant to test activities, for their offices.

The PEO has selected the following OPSEC measures for implementation in ongoing activities and planning for future operations. OPSEC Officers and Coordinators will monitor these OPSEC measures. The process is continuous and will consider the changing nature of critical information, the threat, and vulnerabilities throughout all PEO GCS operations.

### **OPSEC Awareness**

- PEO GCS personnel will maintain compliance with the annual OPSEC and security training.
- The OPSEC Officer or Coordinator will post OPSEC posters throughout facilities and rotate them on a quarterly basis.
- OPSEC awareness efforts will include newsletters, email reminders, bulletins, etc.
- The OPSEC Officer will remind all personnel that the enemy will exploit sensitive photos showing the results of improvised explosive device (IED) strikes, battle scenes, casualties, destroyed or damaged equipment, and killed enemies as propaganda and terrorist training tools.
- The OPSEC Officer will inform all personnel of the danger of unwittingly magnifying enemy capabilities simply by exchanging photos with friends or relatives, or by publishing them on the internet or other media without proper OPSEC review.

### **All Personnel**

- Protect information that may have a negative impact on relations with coalition allies or world opinion.
- Take reasonable steps to minimize risk of access to CUI by unauthorized personnel.

- Avoid displaying CUI in public places (e.g., airports, airplanes, restaurants).
- Avoid open posting of planned schedule notices that reveal when sensitive events will occur.
- Control the issuance of orders, movement of units, programs, or key personnel lists.
- Protect information whenever you leave your desk. Whenever you step away, make a quick check to see whether there is sensitive information on your desk; if so, place it in a secure location off your desktop.
- Be prepared to implement a "clean desk" on 1-hour notice in the event of visitors.
- During periods of increased operational activity, follow the normal leave policy and working hours to the maximum extent possible to preserve the outward appearance of normalcy.
- Ensure that discussions or releases to the media receive an OPSEC review.

### **Waste Disposal**

Throwing information in the trash allows the adversary to retrieve it and gain information about our activities. The trash can is for non-informational items only (e.g., food waste, wrappers).

Destroy classified waste IAW applicable requirements. Use shredders or place unclassified information waste in shred bins located throughout PEO GCS facilities. PEO GCS can shred CDs and DVDs in Building 229, Room 300-W, and the TACOM Life Cycle Management Command (LCMC) G-2 can degauss and destroy hard drives and other media (See [IA BBP 03-PE-O-0003](#)).

### **Conferences and Symposia**

Personnel at conferences and symposia are susceptible to elicitation and exploitation by participants who covertly represent intelligence collection agencies. Without constant awareness of the threat and critical information, personnel may inadvertently release information of analytic value. PEO GCS personnel will complete an annual security briefing to remind them of the threat and of their security responsibilities. Additionally, the OPSEC Officer will make a continuing effort to keep personnel informed, via bulletins and guidance updates, of measures designed to protect sensitive program information and the need for continued awareness and enforcement of OPSEC principles. PEO GCS will attend a threat awareness brief from the local 902<sup>d</sup> Military Intelligence (MI) Group office prior to attending any conference or symposium known to be attended by foreign nationals.

### **Conference Room Security**

The coordinator of any meeting on PEO GCS premises will work with the OPSEC Officer to ensure conference room security. Classified and sensitive information could be compromised by covert listening devices installed in meeting rooms. Unauthorized personnel may also gain entrance to larger meeting rooms and become exposed to information for which they do not have a need to know.

Meetings, briefings and conferences will be held in locations authorized for the proper clarification and sensitivity level.

- The individual responsible for arranging the meeting will be responsible for the security of the meeting. The responsible individual will—
  - Notify the attendees of the classification or sensitivity of the meeting.
  - Prepare the room for classified or sensitive discussion, e.g., unplug telephones, cover windows, clear adjacent rooms, turn off audio or video equipment not needed for the briefing, or ensure attendees were banned from bringing in portable electronic devices (PED).
  - Ensure that each person attending the meeting has the appropriate access authorization by verifying invitee lists and controlling ingress and egress to the room during discussions and after each break.
  - Ensure that notes taken are properly classified and marked and that arrangements have been made for the proper transmission of notes back to each attendee's organization by verification of courier authorization or appropriate electronic transmission. If these measures are not feasible, the responsible individual will ensure that no notes are taken.
  - Ensure that adequate storage facilities are available.
  - Monitor the meeting to ensure that discussions are limited to the level authorized.
  - Sweep the room after the meeting to ensure that no classified or sensitive material has been left behind.
- PEO GCS security personnel will inspect conference rooms used to conduct classified meetings prior to use as part of their routine security procedures. Only conference rooms approved by the Security Manager are authorized for classified discussions.

### **Unsolicited Requests for Information**

Intelligence collectors often use elicitation as a technique to discreetly gather information that could facilitate future targeting attempts. Elicitation techniques are usually non-threatening, easy to disguise, deniable, effective, and usable to obtain information on personnel, military installations, and government facilities. The conversation can be in person, over the phone, or in writing.

Know what information should not be shared, and be suspicious of people who seek such information. Do not tell people any information they are not authorized to know, to include personal information about you, your family, or your colleagues.

You can politely discourage conversation topics and deflect possible elicitations by—

- Referring them to public sources (e.g., websites, press releases)
- Ignoring any question or statement you think is improper and changing the topic
- Deflecting a question with one of your own
- Responding with "Why do you ask?"
- Giving a nondescript answer

- Stating that you do not know
- Stating that you would have to clear such discussions with your security office
- Stating that you cannot discuss the matter.

If you believe someone has tried to elicit information from you, especially about your work, report it to your OPSEC Officer.

### **Compromising Emanations**

Electronic and electromechanical telecommunications and automated information processing equipment can produce unintentional, intelligence-bearing emanations. The study of these emanations is commonly known as TEMPEST. Interception and analysis of these emanations can disclose information transmitted, received, handled, or otherwise processed by the equipment. All Army facilities (including contractor facilities supporting the Army) electronically processing classified information must provide information to the TEMPEST Program Manager for a facility review to determine whether a formal TEMPEST Countermeasure Review (TCR) is required. A PEO GCS Security Manager will oversee these reviews and submission of this information on [DD Form 254](#). If a contractor either receives or generates classified information or material via electronic means (blocks 11b and 11c), then block 11i will be checked YES and include the PEO GCS TEMPEST standard language, which identifies the process for contractors to submit a request for a TEMPEST review.

### **Communications Security**

The Army is very concerned about the vulnerability of voice communications. The threat to the national security is real and it is current. All unsecured telephone conversations are vulnerable to monitoring, and all long-distance microwave transmissions are subject to intercept. Such vulnerabilities provide a rich source of information to intelligence agents. To effectively counter the threat to voice communications, all personnel will take the following OPSEC measures:

Classified or sensitive information will not be discussed over an un-secure telephone or network. Each employee will carefully consider the security implications of any information to be discussed and use only approved secure means to discuss classified or sensitive information. All personnel will use the Secure Telephone Equipment (STE) in the encrypted mode whenever necessary, particularly when discussing any technical information. If an STE is not available, Defense Connect Online (DCO) is an alternate secure option when used with a headset or in a conference room using the conference room security identified above. DCO is encrypted to DoD-mandated levels of security and is housed in DISA's secure computing facilities. DCO is available to anyone with a Common Access Card (CAC) and to individuals sponsored by a CAC holder (with registration). Training is available from a PEO GCS Security Manager for the operation of STE phones and DCO. STEs will only be in restricted access areas, to avoid the compromise of critical information. Use of STEs will comply with the STE User Brief provided by the local COMSEC Custodian.

Personnel will maximize the use of secure communications, telephone, fax, classified email, U.S. Message Text Format messages, or Public Key Infrastructure (PKI) enabled computer networks; and not attempt to “talk around” classified information by using code words, catch phrases, or other double-talk. Taken alone, an individual conversation might not result in a compromise of classified information, but when placed in a sequence of several conversations that may occur over several days, the possibility of compromise becomes very real.

When sending sensitive information via a unsecure facsimile machine, personnel will coordinate the transmission and receipt of information prior to faxing to ensure the information does not remain unattended on the receiving end of the transmission. This coordination should include immediate confirmation of receipt by the recipient upon retrieval of the information.

All personnel will store, use, and destroy issued COMSEC material IAW [AR 380-40](#), Safeguarding and Controlling Communications Security Material, 9 July 2012, and TB 380-41.

All personnel will limit mission-related email to only “.mil” and “.gov” accounts. Transmission of sensitive information or CUI will only be via encrypted email.

### **Computer Security**

The nature of PEO GCS operations requires extensive use of computer equipment. Without adequate security measures, this equipment is susceptible to intrusion or tampering through hardware or software manipulation. Personnel will only process classified information on computer systems that have been approved by the Designated Approval Authority (DAA) IAW [AR 25-2](#) or, in the case of contractor systems, approved by the Defense Security Service (DSS) IAW the National Industrial Security Program Operating Manual ([NISPOM](#)).

In addition, the following measures will protect unclassified sensitive information or CUI:

- Physically protect computer systems from intrusion or tampering by keeping them in PEO GCS facilities.
- Include Data-At-Rest encryption on laptops.
- Avoid processing CUI on public computers (e.g., those available for use by the general public in kiosks, hotel business centers) or computers that do not have access control, including personally owned computers.
- Physically protect mobile devices used to store CUI electronically (e.g., PEDs, removable media) and use [NIST](#) or [NIAP](#)-approved cryptographic products. These are available at [ECA PKI Program](#) or [NIST Security Management & Assurance](#).

## Employee Travel

PEO GCS personnel are susceptible to elicitation and exploitation during travel by individuals who covertly represent the intelligence collection agencies of foreign governments. Collection efforts may range from innocuous questions from friendly inhabitants to actual blackmail by intelligence agents, electronic monitoring, document duplications, and actual theft of material. Without constant awareness of the threat and the CIL, personnel may inadvertently provide sensitive information of analytic value to foreign intelligence agents. The OPSEC Officer will provide periodic security briefings to PEO GCS personnel as part of the continuing OPSEC awareness effort, which also includes bulletins and OPSEC guidance updates of measures designed for the protection of sensitive program information and the need for continued awareness and enforcement of OPSEC principles. OPSEC measures for travel include the following:

- Travel in civilian clothes whenever possible. Do not carry bags or other items that identify you as a member of PEO GCS or the Army.
- Use a passport instead of military orders whenever possible.
- Do not discuss assignments, duties, or reasons for travel unless absolutely necessary (e.g., with security, customs, or immigration personnel).
- Comply with [PEO GCS Policy for Traveling Outside the Continental United States \(OCONUS\) with Government Furnished Equipment \(GCS-12-007\)](#), 7 June 2012.

## Shipment of Sensitive Materials

When shipping sensitive material, personnel will consider the safety of the shipment method and review the label markings for sensitive information. Not only are shipments of sensitive material subject to interception, but labels placed on packaging can sometimes reveal information of analytic value.

## Public Release

Personnel will not discuss, show or make available safeguarded information to unauthorized individuals. The OPSEC Officer will review information, materials, or records IAW [AR 530-1](#) prior to public release. The only approval authority other than the PEO to release PEO GCS information to the public is the PEO GCS PAO. Follow the PEO GCS Public Release process to obtain approval for release of information.

## Website OPSEC Reviews

The internet and intranet allow PEO GCS to further increase distribution of print and broadcast mediums to reach a wider audience. Creators and designers of this material will ensure it meets OPSEC requirements. PEO GCS integrates OPSEC reviews of its websites into the overall OPSEC program and includes it in their annual OPSEC Program Status Report to OSE. The OPSEC Officer will work with the PAO and Webmaster to ensure that website owners do the following:

- Verify a valid mission need to disseminate the information to be posted.
- Vet information via the PEO Public Release process prior to posting information to the website.
- Protect information according to its sensitivity, and ensure reviewing officials and webmasters are selected and have received appropriate training in security and release requirements IAW Army web policy.
- Security Managers, PAOs, and webmasters will use the PEO checklist to review content quarterly on their publicly accessible websites.

## **Employee Disaffection**

Supervisors or fellow employees should report individuals to the PEO Security Office who, through personal adversities or circumstances (e.g., marital difficulties, criminal or non-acceptable social behavior, excessive indebtedness, indiscriminate use of alcohol or drugs) present an attractive target to foreign intelligence agencies. Non-action on the part of personnel who become aware of these situations can be as significant a threat as that presented by a foreign agent who may attempt to exploit personnel experiencing these problems.

## **Document Markings**

All documents containing PEO GCS information will be marked appropriately by the author upon creation. Proper use and application of markings to indicate classification or the presence of CUI are necessary to identify the proper protection and who is authorized to receive the information. Classified information will be marked IAW [DoDM 5200.01, Vol. 3](#), to identify the level of protection and dissemination of the information. CUI is identified in the Security Classification Guides and [DoDM 5200.01, Vol. 4](#), as well as below.

The For Official Use Only (FOUO) designation encompasses unclassified information that is eligible for exemption from mandatory public disclosure under the FOIA. FOUO information includes commercial or financial information generated by or for the Government with the understanding that it is on a privileged or confidential basis (e.g., bids, contracts, proposals, trade secrets, inventions, discoveries, proprietary data, data on contract performance). When identified in the SCG or instructed by the Security Office, material will be marked FOUO. This information is excluded from public release; however, information is not excluded or marked FOUO merely because it is OPSEC sensitive. To qualify for marking as FOUO, information must fall under one or more of the exemption categories specified in [AR 25-55](#), The Department of the Army Freedom of Information Act Program, 1 November 1997. Marking instructions are in the SCG or [AR 25-55](#).

Technical data is any recorded information related to experimental, developmental, or engineering works that can be used to define an engineering or manufacturing process, or can be used to design, procure, produce, support, maintain, operate, repair, or overhaul program material. The data may be graphic or pictorial delineations in media (e.g., computer software, drawings, photographs), text in specifications, related

performance or design documents, or computer printouts. Examples of technical data include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, catalog-item identifications, and computer software documentation. PEO GCS personnel will protect technical data by applying a distribution statement to limit the dissemination of the information. An export control warning notice may also accompany the distribution statement. Marking instructions are in the SCG or [Department of Defense \(DoD\) Instruction 5230.24](#), Distribution Statements on Technical Documents, 23 August 2012.

## **CUI Protection Measures**

CUI protection measures include the following:

- Release CUI only to an individual who is a U.S. person and has a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose.
- Handle CUI material to prevent its disclosure to the general public and to limit its circulation to those employees who need the material to perform their work duties
- Do not leave CUI material unattended when removed from storage.
- After working hours, store CUI information in locked desks, file cabinets, bookcases, locked rooms, or similar means.
- Do not display CUI in public places, such as airports, airplanes, restaurants, etc.
- Do not process CUI on public computers (e.g. those available for use by the general public in kiosks, hotel business centers) or computers that do not have access control, including personally owned computers.
- Protect CUI stored electronically on portable devices (e.g., laptops, personal electronic devices, removable media) physically or by using approved Data-at-Rest.

CUI printed documents and material may be transmitted through mail channels or hand-carried without formal courier orders. FOUO information may be disseminated to DoD personnel and DoD contractors to conduct official business for the program. If dissemination is required outside of DoD personnel or DoD contractors, contact the appropriate Security Manager for approval. Technical data will follow the release instructions identified in the Distribution Statement.

All transmission or dissemination of CUI identified with a Distribution Statement or marked FOUO will use [NIST](#) or [NIAP](#)-approved cryptographic products.

CUI documents may be destroyed by any means approved for the destruction of classified information, i.e., cross-cut shredding or other means that would make it difficult to recognize or reconstruct the information.

## **Visitor Control**

Visitors to PEO GCS offices, areas, and activities may observe or hear sensitive information, operations, or activities. Any person not permanently assigned to PEO

GCS is considered a visitor. Organizations will provide escorts for visitors that need access to restricted areas. Activities of visitors and non-assigned personnel are the responsibility of the escort. Escorts will be knowledgeable of proper escort procedures, limitations of disclosure, and other applicable controls involved in the visit. Most importantly, the escort will have sufficient knowledge of the activity to be performed by the visitor to preclude unauthorized activity from taking place during the visit. The OPSEC Officer will provide briefings to remind PEO GCS personnel of the potential for the inadvertent release of information by visual or oral means when visitors are present.

When a visit involves access to classified information or access to secure areas, escorts will control access consistent with the security clearance and purpose (need to know) of the visit. All visitors will process through established checkpoints for verification of identity, citizenship, personnel security clearances, purpose of visit, issuance of badges, inspection of articles being brought into and out of the facilities, and other measures to assure proper visitor control. Access to classified information is not permitted until identification, security clearance and need-to-know are positively established. In no case will visitors have access to information classified higher than what is indicated on the approval of the specified visit. Organizations will not assign un-cleared personnel to duties that may provide them access to classified information until a security clearance is granted and need to know is established.

### **Escorts for Foreign Visitors**

All foreign visitors (i.e. non-citizens) will have escorts in all PEO GCS facilities. For government facilities, this will be by a U.S. Government employee. The Foreign Disclosure Officer (FDO) will provide an Escort Briefing prior to escorting any foreign nationals.

### **Contractor and Subcontractor Requirements**

The PEO contractors will use OPSEC to protect the organization's critical information. The PEO ICW the OPSEC Officer will be responsible for determining OPSEC requirements when the contract involves sensitive unclassified information.

IAW [ALARACT 015/2012](#), Use of an Antiterrorism and Operations Security in Contracting Cover Sheet for Integrating AT/OPSEC into the Contract Support Process, PEO has developed a process for completing the AT/OPSEC Contract Cover Sheets. This is located on the CIO portal under processes and as well as under Security Portal under processes. PEO requirement packages will use the PEO GCS form and provide it the OPSEC Officer to ensure the document is completed and all signatures obtained and returned to the procuring analyst or contracting officer representative.

Unclassified contracts that require the contractor to access, process, handle or store Controlled Unclassified Information (FOUO or technical data) will define the OPSEC requirements in the contract and the SOW to outline the specific OPSEC needs or to follow and implement the PEO OPSEC Plan. This will include "Guidelines for Protecting Controlled Unclassified Information" as an attachment to the contract. Insert the

paragraph below in the SOW for annual OPSEC training requirement to protect the PEO's CIL. A Contract Data Requirement List (CDRL) may be required. This information (OPSEC requirements, training, and CUI attachment) will be flowed down to subcontractors who access, process, handle, or store CUI information.

All U.S. contractors shall provide annual program specific OPSEC training for all program personnel. New program personnel shall receive OPSEC training within 30 days of program assignment. Annually, contractors shall complete OPSEC training and submit a report, validating 100% completion to the Government Security Office by 30 September. This requirement shall be flowed down to all U.S. subcontractors with access to CUI material.

Classified contracts will use the DD254 to document the OPSEC requirements. Refer to the DD254 Contract Security Standard Language and Process Standard Operating Procedure for complete guidance on OPSEC requirements.

## **Annex A – The Intelligence Collection Threat**

Listed below are some examples of specific types of threats within each of the major categories. Of course, examples cited may pertain to more than one category, e.g., terrorists might use HUMINT, SIGINT, etc. to collect information about their target. The Multidiscipline Counterintelligence Threat Assessment for each PMO is classified and will not be included in this OPSEC Plan, to allow for broader dissemination.

### **Foreign Intelligence Service Threat**

- Human Intelligence (HUMINT) (e.g., recruitment, blackmail, surreptitious entry, phone taps, bugs, unauthorized computer access, etc.)
- Signals Intelligence (SIGINT) (e.g., intercept/exploit communications, computer data, TEMPEST, etc.)
- Imagery Intelligence (IMINT) (e.g., overhead imaging, hand held photography, etc.)
- Measurement and Signature Intelligence (MASINT) (e.g. radar intelligence, infrared intelligence and nuclear intelligence.)
- Open Source Intelligence (OSINT) (e.g., Websites, public releases, newspapers, etc).

### **Terrorist Threat**

- Assassination
- Bombing
- Kidnapping
- Radiological, Biological, Chemical attacks
- Nuclear attacks
- Stand-off weapons attacks/Raids

### **Insider Threat**

- Malicious acts by disgruntled personnel (violence, sabotage)
- Espionage/theft of classified material for adversary
- Unauthorized disclosure of classified material
- Theft of property
- Inadvertent loss of classified material

### **Criminal Threat (Outsider)**

- Violent acts against people
- Theft/destruction of property
- Mob Violence
- Hacking/Cracking of Computer Systems

## Environmental Threat

- Fire
- Storm
- Pollution
- Earthquake
- Flood

## Military Threat

- Nuclear
- Radiological/Biological/Chemical
- Conventional
- Unconventional
- Information Warfare

## Human Intelligence

HUMINT is derived from human sources. To the public, HUMINT remains synonymous with espionage and clandestine activities, but most HUMINT collection is performed by overt collectors such as diplomats and military attaches. HUMINT is the oldest, and still arguably the best, method of collecting information. Until the technical revolution of the mid to late 20<sup>th</sup> century, HUMINT was the primary source of intelligence for all governments. For most nations, it remains the mainstay of their intelligence collection activities. HUMINT includes overt, sensitive, and clandestine activities; and the individuals who exploit, control, supervise, or support these sources.

“Overt” activities are performed openly. Overt HUMINT collectors can include military attaches, diplomatic personnel, and members of official delegations. Overt HUMINT activities may include exploiting unclassified publications, conference materials, and congressional hearings; and debriefing legal travelers who traveled to countries of interest to a nation’s intelligence service.

“Sensitive” HUMINT activities may depend on the same methods as overt activities; however, the sponsor of the activity must not be disclosed. Disclosure of the sponsor’s identity may result in political embarrassment, compromise of other intelligence operations, or security threats to the sponsoring nation.

“Clandestine” HUMINT sources include agents who have been recruited or have volunteered to provide information to a foreign nation, and foreign nationals who successfully infiltrate an organization with a cover story. The latter cases are fairly rare, and generally come to the U.S. under the guise of being political refugees. Once in the U.S., they move into positions that allow them to gather political, technical, or economic information for their governments. According to one estimate, more than 100 countries currently conduct intelligence operations against the U.S. Adversary intelligence organizations place a high priority on the acquisition of scientific and technical

information and target the U.S. because of its preeminence in many technological areas. The U.S. Government, American corporations, and U.S. universities have been targeted by intelligence organizations seeking scientific and technical intelligence. The U.S. hosts more science and technology officials, defense attaches, and identified intelligence officers than any other nation in the world.

Intrusive on-site inspection activities required under some arms control agreements provide a significant opportunity for HUMINT collection at facilities of great importance to U.S. national security. On-site inspection provisions are specified in the Treaty of Intermediate Range Nuclear Forces, the Strategic Arms Reduction Treaty, the Bilateral Agreement between the U.S. and Russia on Chemical Weapons, the Treaty on Conventional Forces in Europe, and the Anti-Ballistic Missile Treaty. In addition, the Peaceful Nuclear Explosions Treaty, the Threshold Test Ban Treaty, and the Open Skies Treaty provide the opportunity to gather information from sensitive installations, even though they do not mandate intrusive on-site inspections. These treaties provide for the use of technical collection capabilities to verify national declarations. The operation of these collection systems requires a significant number of support personnel, and some of these personnel are likely to be intelligence collectors. Intelligence collectors in on-site inspections will be accredited inspectors who are specially trained to collect specific types of data and enjoy diplomatic immunity. It is likely that these personnel will try to obtain intelligence through observation of facilities, elicitation of information from escorts and facility personnel, and collection of available documentation.

Even with the explosion of technical capabilities, HUMINT can still provide information that even the most proficient technical collectors cannot, such as access to internal memoranda and to compartmented information. Most importantly, human collectors can provide key insights into the intentions, successes, failures, and weak points of an adversary, whereas technical collection systems are often limited to determining apparent capabilities. HUMINT can reveal adversary plans and intentions, or uncover scientific and weapons developments before they are used or are detected by technical collection systems. HUMINT can also provide documentary evidence such as blueprints of facilities, copies of adversary plans, or copies of diplomatic or policy documents. Finally, HUMINT is extremely cost-effective compared with technical collection systems and does not require a significant technological production base for support.

### **Signals Intelligence**

SIGINT is derived from signal intercepts. It includes all communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT), however transmitted.

COMINT includes information derived from intercepted communications transmissions. COMINT targets voice and tele-printer traffic, video, Morse code traffic, or even facsimile messages. COMINT collectors can harvest it from the air waves, cable, fiber optics, or any other transmission medium.

ELINT includes the interception and analysis of non-communications transmissions, such as radar. ELINT is used to identify the location of an emitter, determine its characteristics, and infer the characteristics of supported systems.

FISINT consists of intercept of telemetry from weapons systems as they are being tested. Telemetry units provide designers with information of a prototype's guidance system operations, fuel usage, staging, and other parameters vital for understanding operational characteristics. This data enables the designer to evaluate the performance of the prototype; however, if intercepted, it also provides an adversary with the ability to estimate the capability of the prototype.

SIGINT collectors can perform collection from a variety of platforms. Examples include overt ground collection sites (e.g., the Russian facility at Lourdes, Cuba; ships; aircraft) and covert locations inside or outside the U.S. SIGINT facilities can monitor transmissions from communications satellites and terrestrial facilities. This is particularly important because many international transmissions originating in the U.S. depend on communications satellites for passage overseas. Communications satellites supporting the transmission of U.S. Government, private sector, and public communications include the International Maritime Satellite System, the International Telecommunications Satellite System, and the European Satellite System. International communications satellites are routinely monitored by foreign intelligence services, including the Russian and Chinese intelligence services. The majority of collection capabilities targeting the U.S. are either ground- or sea-based, and target line-of-sight or satellite communications systems. Space-based collection systems can also collect COMINT, FISINT, and ELINT.

### **Measurement and Signatures Intelligence**

MASINT is scientific and technical intelligence information obtained by quantitative and qualitative analysis of data derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source emitter or sender. This information then facilitates subsequent identification or measurement of the same type of equipment. The term "measurement" refers primarily to the data collected for the purpose of obtaining finite metric parameters. The term "signature" refers primarily to data indicating the distinctive features of phenomena, equipment, or objects as the collection instrument senses them. The signature is used to recognize the phenomenon, equipment, or object when its distinctive features are detected.

MASINT disciplines include radar intelligence (RADINT), infrared intelligence (IRINT), and nuclear intelligence (NUCINT). Because it works in different parts of the electromagnetic spectrum, MASINT detects information patterns not previously exploited by other sensors. MASINT sensors collect information generally considered by the targeted nation to be peripheral in nature. As a result, countermeasures often do not protect these signatures.

## Imagery Intelligence

IMINT is a product of imagery analysis. Imagery includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. IMINT collectors can derive imagery from visual photography, radar sensors, infrared sensors, lasers, and electro-optics. IMINT includes the exploitation of data to detect, classify, and identify objects or organizations. It can be produced from either hard-copy (film) or soft-copy (digital) imagery. Users can analyze and interoperate either type of imagery source for various purposes.

The proliferation of space-based imagery systems permits a much greater use of imagery products by nations that previously did not have access to them. Currently, intelligence services can purchase imagery from a variety of sources. These systems include the Landsat Multispectral Imagery System operated by the U.S., the French SPOT MSI and Pan-chromatic Imaging System, the European Space Agency's ERS-1 Synthetic Aperture Radar Imaging System, and the Japanese JERS-1 multi-sensor imager. Additionally, Russia sells 2-meter or better imagery from its space-based reconnaissance systems.

The commercial imagery market is likely to continue to grow at a high rate, and additional collection systems are always being developed. These will include imaging systems produced by U.S. companies that will be capable of producing 1-meter resolution electro-optical digitized imagery. One-meter imagery is sufficient to conduct technical analysis of terrain, determine key facilities in an urban area, and conduct detailed analyses of industrial facilities. Other nations such as France, Germany, Japan, and Canada are producing advanced imagery platforms that could be used to target sensitive facilities. The growing availability of sophisticated imagery workstations and analytical tools will allow adversaries to conduct more in-depth analysis for targeting and technical intelligence gathering.

The 1992 Open Skies Treaty also resulted in an imagery collection threat. The treaty establishes a regime of unarmed aerial observation flights over the entire territory of its signatories. The treaty was negotiated between the members of NATO and the former Warsaw Pact as a means to promote openness and transparency of military forces and activities. Observation flights can include aircraft provided by the observing nation, the observed nation, or a third participating party. Aircraft can have panoramic and framing cameras capable of ground resolution of no better than 30 centimeters, video cameras with a ground resolution of no better than 20 centimeters, infrared line scanning devices with ground resolution of no better than 50 centimeters, and synthetic aperture radar systems with impulse response rate resolutions no better than 3 meters. Ground resolutions of 50 centimeters or less provide significant detailed information for an imagery analyst. Using the imagery derived from Open Skies flights, analysts can identify particular types of equipment by type and capability, and perform detailed analyses of rail, port, industrial, and military facilities.

Imagery provides significant benefits to an adversary collecting intelligence against the U.S. Properly matured imagery can provide geo-location accuracies for weapons

systems targeting, or other intelligence collection platforms. Imagery further allows activity to be detected, target characteristics to be studied in detail, and equipment and facilities to be enumerated. Further, imagery sensors for mapping of areas of key importance can cover large areas.

Imagery also has limitations. Except for synthetic aperture radar, imagery quality is normally degraded by darkness and adverse weather. This allows the targeted organization to use these periods of time to conduct activities that it wants to go unobserved. If an organization is aware that it is being targeted by imagery systems, it can use camouflage, concealment, and deception (CC&D) techniques to obscure activities or provide a misleading image to the observing party. Effective use of CC&D may result in the adversary drawing erroneous conclusions about the observed organization's capabilities and activities. Finally, imagery intelligence collection usually requires a technologically oriented infrastructure. While this requirement may be reduced to some extent in the future, effective use of imagery will still require well-educated, technically competent analysts—a capability that may be beyond some U.S. adversaries.

### **Open Source Intelligence**

OSINT involves the use of materials available to the public by intelligence agencies and other adversaries. According to the Al Qaeda training manual, 80 percent of its intelligence was from open sources. With the proliferation of electronic databases, it has become easier to collate large quantities of data and structure information to meet the needs of the adversary collector. Open source information can provide extremely valuable information concerning activities and capabilities. Frequently, open source material can provide information on organizational dynamics, technical processes, and research activities not available in any other form. When open source data is compiled, it is often possible to derive classified data or trade secrets. This is particularly true in the case of studies published in technical journals. Analyzing journal articles published by different members of a research organization can often derive a significant understanding of research and development efforts. Finally, open source information is generally more timely and may be the only information available in the early stages of a crisis or emergency.

OSINT collection has limitations. Articles in military or scientific journals often represent a theoretical or desired capability rather than an actual capability. Censorship may also limit the publication of key data needed to arrive at a full understanding of an adversary's actions. Organizations may use the press as part of a conscious deception effort.

### **Computer Intrusion for Collection Operations**

It is unclear to what extent foreign intelligence services are using computer hackers to obtain proprietary data or sensitive government information, or whether they have developed the capability to use computer intrusion techniques to disrupt communications activities. The KGB did, however, sponsor computer intrusion activities

by the Hanover Hackers, and there is no reason to believe that these efforts have ceased. The Hanover Hackers were able to access at least 28 Government computer systems, obtain data from them, and sell it to the KGB. While none of this data was classified, much of it was sensitive, and classified information could potentially have been derived from comparing this information with other data. The KGB has allegedly been involved in similar efforts with other hacker groups and that these operations included remote introduction of logic bombs and other malicious code. The Russian GRU (military intelligence) and SVR (foreign intelligence service) have continued where the KGB left off in this area. There is little doubt that many foreign intelligence services could obtain these capabilities if they wished. The ability of a group of Dutch hackers to obtain sensitive information from U.S. Army, Navy, and Air Force computer networks during Operations Desert Shield and Desert Storm serves as an example of this potential for access. Between April 1990 and May 1991, this group penetrated computer systems at 34 different facilities. The group obtained information on logistics operations, equipment movement schedules, and weapons development programs. Information from one of the penetrated computer systems directly supported Desert Shield and Desert Storm operations. In a review of this incident, the General Accounting Office concluded that a foreign intelligence service would have been able to derive significant understanding of U.S. operations in the Persian Gulf from the information that the Dutch hackers were able to extract from DoD information systems.

## **Terrorism**

A terrorist threat assessment must consider both domestic and international elements. Subsequently, the potential collection threat significantly increases by virtue of the continuous media interest in the organization's activities. No terrorist threat has been identified that specifically targets PEO activities, but various factors present a favorable climate for terrorist activities.

## **Technology Transfer**

There continues to be increasing concern within DoD and the civilian marketplace over the growing challenges to the U.S. lead in military and other types of technology. Technology with military application is a high priority target for all foreign intelligence collection organizations. In their efforts to satisfy their collection requirements, foreign intelligence agents target Government and military organizations, the defense contracting industry, and the academic community. In recent years, there has been a dramatic increase in the emphasis on the collection of high technology weapons systems information and the requisite production technology. This threat should be of particular concern to PEO GCS personnel because we deal with the very weapons systems and operations in which foreign intelligence organizations are interested. When we fail to provide dissemination restrictions on documents; comply with and enforce export control restrictions; or conduct OPSEC reviews of various papers proposed for public media release and presentations, we are indirectly subsidizing foreign weapons development by providing foreign countries and adversaries with new technology for their own systems, as well as assisting them in developing countermeasures for use against U.S. systems and items now in development. Per Department of Defense

Directive ([DoDD](#)) [5230.25](#), Withholding of Unclassified Technical Data From Public Disclosure, Change 1, 18 August 1995, Section 4.2, “Because public disclosure of technical data subject to this Directive is tantamount to providing uncontrolled foreign access, withholding such data from public disclosure, unless approved, authorized, or licensed in accordance with export control laws, is necessary and in the national interest.”

### **Professional Conferences and Symposia**

During attendance at conferences and symposia, personnel are susceptible to elicitation and exploitation by participating individuals (including persons from allied countries) who unwittingly or covertly represent the intelligence collection agencies of foreign governments. Collection efforts may range from innocuous questions from foreign personnel to actual blackmail by foreign intelligence agents. Without constant awareness of the threat, PEO GCS personnel may inadvertently release sensitive information of analytic value.

### **Personnel Disaffection**

Disaffection poses a potential collection and physical threat to PEO GCS. Theft of information or material, altering data, sabotage, espionage, or contamination or destruction of critical materials or equipment could cause serious damage to programs or loss of public confidence in operations.

## Annex B – Vulnerability Assessment

Vulnerabilities are friendly actions that provide indicators that may be obtained and accurately evaluated by an adversary to provide a basis for effective decision making. Vulnerabilities include stereotyped actions that habitually occur (patterns), and unique detectable characteristics that identify the type of activity or intention (signatures). An OPSEC vulnerability exists when the adversary can 1) collect an indicator of critical information, 2) correctly analyze the information, 3) make a decision, and 4) take timely action to adversely influence, degrade, or prevent friendly operations.

The OPSEC Officer in coordination with PEO GCS staff has compared adversary collection capabilities against PEO GCS activities and determined that the following vulnerabilities, if detected by an adversary, could be used to the disadvantage of PEO GCS activities, and that OPSEC measures must be established to protect these potential OPSEC vulnerabilities:

### Information Security Vulnerabilities

- Failure to ensure that classified or sensitive unclassified information is furnished or disclosed only to authorized personnel.
- Failure to provide a security review for classified information resulting in inadvertent disclosure of classified information.
- Employment of un-cleared personnel to duties that may provide the opportunity for access to classified information.
- Failure to follow security classification guidelines for classification of data.
- Failure to maintain security at classified meetings, conferences, or planning sessions.
- Failure to secure classified storage containers and closed areas.
- Failure to follow published security guidance or regulations.
- Failure to follow classification management procedures.
- Failure to protect classified and sensitive unclassified equipment and material.
- Failure to prevent inadvertent release of sensitive information to personnel not having the proper need to know.
- Failure of planners to determine the threat or risk prior to beginning any activities.

### Operations Security Vulnerabilities

- Open sources whereby documents are published and distributed without OPSEC reviews or limited distribution statements.
- Classified documents generated within PEO GCS that are not reviewed for proper marking and handling instructions or compliance with an SCG.
- Improper disposal of sensitive, unclassified information.
- Lack of awareness as to the adversary collection threat, causing personnel to become careless in their day-to-day OPSEC and other security responsibilities.
- Failure to adequately review security requirements during planning and testing.

- Interception of discussion over non-secure communications involving sensitive information regarding current or future operations.
- Military blogs that post sensitive photographs to the internet (e.g., results of IED strikes, battle scenes, casualties, destroyed or damaged equipment).
- Military blogs that provide information that enhances the adversary's targeting process.

## **Physical Security Vulnerabilities**

- Failure to maintain or enforce access controls for controlled or restricted areas.
- Failure to maintain key and lock accountability to facilities that contain PEO GCS information.
- Failure to follow procedures for test and maintenance of intrusion detection systems.
- Failure to follow established procedures in the control and movement of vehicles entering or leaving restricted areas.
- Failure to maintain a positive control system for packages, material, and property into or out of secure areas.
- Failure to comply with physical security standards applicable to designated security areas.
- Failure to use authorized locking devices IAW the sensitivity of the item or information being protected.
- Failure to implement physical security measures at all PEO GCS locations.

## **Information System Vulnerabilities**

- Human error that results in the accidental destruction, disclosure, or modification of sensitive and classified computer-based information.
- Lack of proper use of encryption requirements for transmission of CUI.
- Processing classified or sensitive data on an information system (IS) that has not been approved or accredited for such information.
- Computer transmissions that could be intercepted, causing an unauthorized disclosure of sensitive data.
- Unauthorized persons who may obtain access to the IS, especially when remote dial-in is allowed.
- Improper controls on maintenance personnel prior to allowing them access to IS, to include improperly qualified escorts accompanying and observing performed maintenance.
- Improper control of passwords.
- Improper administrator controls and firewall protection.
- Lack of adequate encryption capabilities.
- Insufficient training in security features and requirements for system administrators.
- Lack of anti-virus and patches.
- Lack of use of Data-at-Rest, and laptop is stolen.

## Annex C – PEO GCS OPSEC Program Matrix

REQUIREMENTS	PEO/PJM	OPSEC Officer	PAO	Webmaster	All Personnel	REFERENCE: AR 530-1
Establish active and documented OPSEC program	X					Paragraphs 2-3. a. (3) and 3-1
Appoint OPSEC Officer in writing	X					Paragraphs 2-3. a. (1) and 3-2. a
Develop, organize, and administer OPSEC program		X				Paragraph 3-2. a. (1)
Ensure that appointed OPSEC Officer receives appropriate training	X					Paragraphs 2-3. a. (2), 3-2 (4) and 4-2. b.
Provide guidance and oversight to multiple subordinate OPSEC programs of various PM organizations		X				Paragraph 3-2. a. (1)
Write OPSEC Plan		X				Paragraphs 2-3. a. (3), 3-2 and 3-2. c.
Develop and propose CIL/EEFI for approval		X				Paragraph 2-3. a. (5)
Approve CIL/EEFI	X					Paragraph 2-3. a. (5)
Conduct initial OPSEC Awareness Training for all newly assigned personnel 30 days of arrival		X				Paragraph 4-2. a. (1)
Conduct continuous OPSEC Awareness Training		X				Paragraph 4-2 a. (2) (a) (b)

<b>REQUIREMENTS</b>	<b>PEO/PJM</b>	<b>OPSEC Officer</b>	<b>PAO</b>	<b>Webmaster</b>	<b>All Personnel</b>	<b>REFERENCE: AR 530-1</b>
Receive annual OPSEC Awareness Training					X	Paragraph 4-2 a. (2) (b)
Conduct OPSEC Reviews		X				Paragraph 5-1
Conduct OPSEC website reviews		X	X	X		Paragraphs 2-2. c. & 5-2. d. (2)
Compare identified indicators with adversary intelligence collection capabilities		X				Paragraph B-3. b. (1).
Conduct analysis of vulnerabilities		X				Paragraph 3-2. b. (1) (c)
Conduct OPSEC assessments		X				Paragraph 5-4
Determine OPSEC requirements when contract involves sensitive information		X				Chapter 6
Consider OPSEC in all activities	X	X	X	X	X	Paragraph 1-8. b.
Decide which OPSEC measures to recommend for implementation and when to do so		X				B-5. b.
Approve OPSEC measures	X					B-6. a.
Implement OPSEC measures	X	X	X	X	X	B-6
Evaluate effectiveness of OPSEC measures during execution		X				B-6. b.

## Annex D – OPSEC Checklist

<b>ALL PURPOSE CHECKLIST</b>		PAGE 1 OF 2 PAGES		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA		DATE		
<b>OPERATIONS SECURITY (OPSEC) CHECKLIST</b>				
NO	ITEMS	YES	NO	N/A
<b>RESPONSIBILITIES</b>				
1.	Does the organization/activity have a written OPSEC program down to PMO level? ( <a href="#">AR 530-1</a> , 2-3. a.)			
2.	Does the organization/activity have a written OPSEC Plan to protect sensitive and critical information? ( <a href="#">AR 530-1</a> , 3-2)			
3.	Has an OPSEC Officer been appointed in writing? ( <a href="#">AR 530-1</a> , paragraph 3-2. a.)			
4.	Are the OPSEC Officers and Coordinators knowledgeable of their duties? ( <a href="#">AR 530-1</a> , Appendix H)			
5.	Has the appointed OPSEC officer attended the HQDA OPSEC Officer Level II certification course conducted by the Army OPSEC Support Element (OSE)? ( <a href="#">AR 530-1</a> , 4-2. b.)			
6.	Has the PEO/PM established OPSEC as a PEO/PM emphasis item and included OPSEC effectiveness as an evaluation objective for all operations, exercises, and activities? ( <a href="#">AR 530-1</a> , 2-3. a. (12))			
7.	Has the PEO/PM approved the organization's CIL? ( <a href="#">AR 530-1</a> , 2-3. a (5))			
8.	Do all personnel (including military, DA Civilians, and DoD contractors) receive Initial OPSEC Awareness Training within the first 30 days of arrival in the organization? ( <a href="#">AR 530-1</a> , 4-2 a. (1))			
9.	Does the OPSEC training program include Continuous OPSEC Awareness Training? ( <a href="#">AR 530-1</a> , 4-2. a. (2))			

NO	ITEMS	YES	NO	N/A
10.	Does each individual know the answers to the following questions? ( <a href="#">AR 530-1</a> , 4-2. a. (1)) <ul style="list-style-type: none"> <li>a. What is my unit or organization’s critical information?</li> <li>b. What critical information am I personally responsible for protecting?</li> <li>c. How is the threat trying to acquire my critical information?</li> <li>d. What steps am I/are we taking to protect my/our critical information?</li> <li>e. Who is my OPSEC Officer?</li> </ul>			
11.	Does the PEO/PM submit the Annual OPSEC Report through higher headquarters for the Fiscal Year (FY) to the OSE? ( <a href="#">AR 530-1</a> , 2-4. d.)			
	<b>Websites</b>			
12.	Does the PEO/PM comply with Federal, DoD, and DA website administration policies and implementing content-approval procedures that include OPSEC and PAO reviews before updating or posting information on all websites? ( <a href="#">AR 530-1</a> , 2-3,a.(15))			
13.	Are quarterly reviews of public websites being conducted to ensure compliance with AR 25-1 and the content is relevant and appropriate? ( <a href="#">AR 530-1</a> , 2-3,a.(15)(a))			
	<b>FOIA, Privacy Act, and Contracts</b>			
14.	Do responses to Freedom of Information Act (FOIA) or Privacy Act requests receive OPSEC review? ( <a href="#">AR 530-1</a> , 5-2)			
15.	Is OPSEC incorporated into all classified contracts as well as unclassified contracts that involve sensitive information? ( <a href="#">AR 530-1</a> , 2-3.a.(11) and 6–2)			
16.	Is OPSEC considered for all contract requirement packages IAW <a href="#">ALARACT 015/2012</a> ?			
	<b>PAO</b>			
17.	Is OPSEC considered in all public affairs planning and execution procedures in support of antiterrorism efforts? ( <a href="#">AR 525-13</a> , Appendix C-4.d (4))			

NO	ITEMS	YES	NO	N/A
18.	Does the staff office or agency providing information, materials, or records to the PA office for release conduct OPSEC reviews? ( <a href="#">AR 360-1</a> , 5-4)			
19.	Do creators and designers of Internet and Intranet material ensure that it meets OPSEC requirements? ( <a href="#">AR 360-1</a> , 5-6 c (4))			

## Annex E – Terms

<b>Adversary</b>	Those individuals, groups, or organizations that must be denied critical information to maintain friendly mission effectiveness. Adversaries may include hostile countries, terrorists, and allied intelligence agencies.
<b>AR</b>	Army Regulation
<b>CIL</b>	Critical Information List
<b>Collection Threat</b>	Adversaries may collect information on U.S. Army activities using various intelligence collection methods. These pieces of information provide an accurate portrayal of the organization's overall intentions or operations.
<b>C2</b>	command and control
<b>C2W</b>	command and control warfare
<b>COMSEC</b>	Communications Security. A type of information or material controlled and managed under a separate set of security standards and procedures from those that apply to other classified information. The loss of COMSEC information or material can seriously damage the national interest.
<b>Critical Information</b>	Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act to guarantee the failure of friendly mission accomplishment.
<b>CUI</b>	Controlled Unclassified Information. Types of information that are not classified but require protective measures which restrict its distribution for a variety of reasons. The types of information considered CUI for PEO GCS are information marked "For Official Use Only" and Technical Data.
<b>DA</b>	Department of the Army
<b>DAA</b>	Designated Approval Authority. A position defined by Department of Defense Directive (DoDD) <a href="#">8500.01E</a> , Information Assurance (IA), 24 October 2002.
<b>DCO</b>	Defense Connect Online
<b>DoD</b>	Department of Defense

<b>DSS</b>	Defense Security Service. Provides the military services, defense agencies, federal agencies, and cleared contractor facilities with security support services.
<b>Essential Secrecy</b>	The condition achieved from the denial of critical information to adversaries.
<b>FOIA</b>	Freedom of Information Act. Allows people to gain access to non-classified information from government agencies.
<b>Foreign Visitor</b>	A person who was born outside the jurisdiction of the United States, is a citizen of a foreign government, and has not been naturalized under U.S. law.
<b>FOUO</b>	For Official Use Only. Unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act.
<b>HUMINT</b>	Human Intelligence. Collection of information by human sources for intelligence purposes. Gathered covertly by espionage agents, or overtly through information available to the general public, it is the most basic form of intelligence collection. HUMINT remains significant because it is often the only source with access to an opponent's intentions and plans.
<b>IMINT</b>	Imagery Intelligence. Collection of information by photographic, infrared, or radar imagery. Images can be gathered by individuals or by remote means, such as aircraft or satellite. This method is valuable because it provides analysts with clues to other areas requiring examination. IMINT includes unauthorized duplication of documents.
<b>Indicators</b>	Friendly detectable actions and open source information that can be interpreted or pieced together by an adversary to derive critical information.
<b>IS</b>	Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
<b>IO</b>	Information Operations
<b>MASINT</b>	Measurement and Signature Intelligence. Scientific and technical intelligence obtained by quantitative and qualitative analysis of data derived from technical sensors to identify distinctive features associated with the source, emitter, or sender. It is technical in nature.

<b>Military Deception</b>	Actions executed to mislead foreign decision makers, causing them to derive and accept desired appreciation of military capabilities, intentions, operations, or other activities that evoke foreign actions that contribute to the originator's objectives. Deception is an effective OPSEC measure that can be employed given prior coordination (e.g., cause adversary intelligence collection efforts to fail to target friendly activities, create confusion or misinterpretation of information obtainable from open sources).
<b>NIAP</b>	National Information Assurance Partnership. A program to increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and validation programs.
<b>NISPOM</b>	National Industrial Security Program Operating Manual. Establishes standard procedures and requirements for government contractors with regards to classified information.
<b>NIST</b>	National Institute of Standards and Technology. Promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.
<b>Observables</b>	Actions that convey indicators exploitable by adversaries but that must be carried out to plan, prepare for, or execute activities.
<b>OPSEC</b>	Operations Security. A program meant to deny our adversaries access to any critical information.
<b>OPSEC Compromise</b>	Disclosure of sensitive or critical information that has been identified by the PEO or any higher headquarters as jeopardizing the ability of PEO GCS to execute its mission or to adequately protect its personnel or equipment.
<b>OPSEC Measure</b>	Methods and means to gain and maintain essential secrecy about critical information.
<b>PAO</b>	Public Affairs Office
<b>PKI</b>	Public Key Infrastructure
<b>PMO</b>	Project Management Office
<b>Publicly Accessible Website</b>	Any DoD website with access unrestricted by password or PKI authorization. "Public" refers to the at-large audience on the Internet, i.e., anyone who can access a website with a browser.

<b>TARP</b>	Threat Awareness and Reporting Program
<b>Sensitive Information</b>	Any information, the loss, misuse, or unauthorized access to, or modification of which could adversely affect the national interest or the conduct of Federal programs, but that has not been specifically authorized under an Executive Order or an act of Congress to be kept secret in the interest of national defense or foreign policy.
<b>SIGINT</b>	Signals Intelligence. Collection of information by interception of electronic signals from communications equipment or non-communicative devices that emit an electronic signal, such as a radar beacon. It includes interception of communication and the interception and analysis of communication between pieces of equipment (e.g., computer networks).
<b>Vulnerabilities</b>	Friendly actions that provide indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making. Vulnerabilities exist when three conditions exist: 1) adversary has capability to collect indicator, 2) adversary has time to process (report, analyze, take planning action), and 3) adversary is able to react.

## Annex F – References

1. [Uniform Code of Military Justice](#)
2. [AR 530-1, Operations Security](#)
3. [AR 25-2, Information Assurance](#)
4. [AR 525-13, Antiterrorism](#)
5. [AR 360-1, The Army Public Affairs Program](#)
6. [AR 381-12, Threat Awareness and Reporting Program](#)
7. [AR 380-40, Safeguarding and Controlling Communications Security Material](#)
8. [DoD 5220.22-M, National Industrial Security Program Operating Manual](#)
9. [DoDM 5200.01, DoD Information Security Program](#)
10. [AR 25-55, The Department of the Army Freedom of Information Act Program](#)
11. [Department of Defense \(DoD\) Instruction \(DoDI\) 5230.24, Distribution Statements on Technical Documents](#)
12. [ALARACT 015/2012, Use of an Antiterrorism/Operations Security \(AT/OPSEC\) in Contracting Cover Sheet for Integrating AT/OPSEC into the Contract Support Process](#)
13. [DoD Directive \(DoDD\) 5230.25, Withholding of Unclassified Technical Data From Public Disclosure, Change 1](#)