III CORPS & FORT HOOD REGULATION 530-1

Operations Security

OPSEC Program

Department of the Army

Headquarters, III Corps and Fort Hood

Fort Hood, TX 76544

17 February 2017

UNCLASSIFIED

SUMMARY OF CHANGE

Fort Hood Regulation 530-1
Operations Security Program

This is a Major Revision dated 17 February 2017

- Changed the Title Page to reflect the new chapters and Appendices.
- Updated Appendix A (References).
- Added the Process Sample to Appendix B (The Operations Security Program Process).
- Added the new checklist to Appendix I (Operations Security Program Assessments).
- Added Appendix J (Website Review).
- Added Appendix K (Quarterly Reporting).
- Added Appendix L Operations Security (OPSEC) Compromise Reporting Procedures.

DEPARTMENT OF THE ARMY ***III CORPS & FH REG 530-1**
HEADQUARTERS, III CORPS AND FORT HOOD
FORT HOOD, TEXAS 76544-5000
17 FEBRUARY 2017

Operations Security (OPSEC) Program

History. This version is a revision. Portions affected by this regulation are listed in the summary of change.

Summary. This regulation codifies the III Corps and Fort Hood Operations Security (OPSEC) Program.

Applicability. This regulation applies to all military personnel, Department of the Army (DA) Civilian employees, and DoD contractors assigned or attached to, or employed by activities, units, and/or tenant agencies at Fort Hood. This policy remains in effect until changed or revoked by this Headquarters (HQ).

Supplementation. Supplementation of this regulation is prohibited without approval from the Directorate of Plans, Training, Mobilization, and Security (DPTMS), Plans and Operations Division.

Suggested Improvements. The proponent of this regulation is Chief, DPTMS, Plans and Operations Division. Send comments and suggested improvements to the Chief, DPTMS, ATTN: IMHD-PLO, Fort Hood, Texas 76544.

FOR THE COMMANDER:

JOHN W. REYNOLDS
COL, GS
Chief of Staff

Official:

CHARLES E. GREEN, SR

Director, Human Resources

DISTRIBUTION:

IAW FH Form 1853: S

*This publication supersedes Fort Hood Regulation 530-1, dated 25 February 2014

Contents

Chapter 1
Introduction, page 1
Purpose, 1-1, page 1
References 1-2, page 1
Explanation of Abbreviations and Special Terms, 1-3, page 1
Responsibilities, 1-4, page 1
Definitions, 1-5, page 1
Requirement, 1-6, page 3
Application, 1-7, page 3
Proponent, 1-8, page 4

Chapter 2
Responsibilities, page 5
All Personnel, 2-1, page 5
Commanders at All Levels, 2-2, page 6
Commanders of Units, Activities, Directorates at Battalion, and Higher Echelons, 2-3, page 7
Garrison Commander, 2-4, page 9
Fort Hood OPSEC Program Manager, 2-5, page 10
Installation Support Directorates, 2-6, page 11
Installation Support Offices, 2-7, page 11
Public Affairs Office (PAO), 2-8, page 11
Organization Webmasters, 2-9, page 12
Freedom of Information Act (FOIA) Officer, 2-10, page 12

Chapter 3
Policy and Procedures, page 12
General, 3-1, page 12
OPSEC Programs, 3-2, page 13
Program Awareness and Training Product Promotion, 3-3, page 14
Threat analysis support to OPSEC, 3-4, page 15

Chapter 4
Training Requirements, page 15
Overview, 4-1, page 15
Training Levels, 4-2, page 15
Additional Training, 4-3, page 17
Joint and Interagency Training, 4-4, page 18

Chapter 5
OPSEC Review, Assessment and Survey, page 19
Section I
OPSEC Review, page 19
General, 5-1, page 19
Procedures, 5-2, page 19
Section II
OPSEC Assessment, page 20
General, 5-3, page 20
Procedures, 5-4, page 20
Section III
OPSEC Survey, page 21
General, 5-5, page 21
Procedures, 5-6, page 21

Chapter 6
OPSEC Contract and Subcontract Requirements, page 22
Overview, 6-1, page 22
Policy and Procedures, 6-2, page 22

Chapter 7
Special Access Programs (SAP), page 24
Overview, 7-1, page 24
Policy, 7-2, page 24

Appendixes
A. References, page 24
B. The OPSEC Process, page 28
C. Critical Information List, page 35
D. OPSEC Indicators, page 36
E. The Threat, page 41
F. Sample OPSEC Measures, page 45
G. OPSEC Relationships to Security Programs, page 48
H. Duty Description for OPSEC Officers and Eligibility Requirements, page 51
I. Program Assessments, page 55
J. Website (WS) Review Checklist, page 57
K. Quarterly Reporting, page 59
L. Compromise Reporting Procedures, page 60

Tables:
Table B-1:The Five-Part OPSEC Process Worksheet Sample, page 34
Table I-1: OPSEC Assessment Checklist, page 56
Table J-1: Website Review Checklist, page 57

Figures
Figure K-1: Officer Roster, page 59
Figure K-2: Level I Training Statistics, page 60

Glosary
Section I, page 62
Abbrevations page, 62
Section II, page 71
Terms, page 71

Chapter 1
Introduction

1-1. Purpose

a. This regulation documents the policies and procedures needed to meet the specific OPSEC program requirements of Fort Hood and support the OPSEC programs of higher echelons.

b. This publication specifically addresses the common features of a functional, active, and documented OPSEC program. Each separate entity of the command may require a unique approach to OPSEC depending upon the function of the organization. The basic concepts set forth herein are essentially the same for every organizational element of the command. OPSEC is applicable to all activities within the command, from the daily routine planning, testing, exercise, and evaluation phases; through force mobilization, validation, deployment, recovery, and reconstitution.

c. The overall purpose of OPSEC is to strengthen our traditional security procedures by identifying existing vulnerabilities or weaknesses and applying measures to preserve essential secrecy in every phase of operations, tests, exercises, or activities. This OPSEC publication will identify and discuss the five-step process: Identify Critical Information, Analyze Threats, Analyze Vulnerabilities, Assess Risk, and the Apply OPSEC Measures.

d. OPSEC applies to all activities on the Fort Hood installation. An adversary can learn a lot about our plans and programs by piecing together observable or obtainable unclassified information. Therefore, in an attempt to shield our activities, it is not only important to follow normal security procedures, but also to implement OPSEC measures as needed.

1-2. References

Required and related publications are listed in Appendix A.

1-3. Explanation of Abbreviations and Special Terms

Abbreviations and special terms used in the regulation are explained in the glossary.

1-4. Responsibilities

Responsibilities are listed in chapter two. Responsibilities referring to commanders and similar terms are equally applicable to equivalent management and supervision positions in organizations that do not employ a traditional military structure.

1-5. Definitions

a. OPSEC

(1) As defined in Department of Defense (DOD) OPSEC Program (Department of Defenese Directive(DoDD) 5205.02E), OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations, as well as other activities to:

(a) Identify those actions that can be observed by an adversary intelligence system.

(b) Determine indicators and vulnerabilities that adversary intelligence systems might be able to obtain. Data that could be interpreted or pieced together to derive critical information that over time could be useful to adversaries and represent an unacceptable risk.

(c) Select and execute countermeasures that eliminate or reduce risk to a level acceptable by the commander.

(2) OPSEC protects Sensitive and/or Critical Information (S/CI) from adversary observation and collection in ways that traditional security cannot. While programs such as Information Assurance (IA) protect classified information, they cannot prevent all indicators of critical information, especially unclassified indicators, from being revealed.

(3) In concise terms, the OPSEC process identifies the critical information of military plans, operations, and supporting activities, as well as the indicators that reveal it. Once identified, measures must eliminate, reduce, or conceal those indicators. During the process, a determination must be developed for when the information may cease to be critical in the lifespan of an organization's specific operation.

b. Critical Information

(1) Critical information is defined as information important to the successful achievement of United States (U.S.) objectives and missions, which may be of use to an adversary of the U.S.

(2) Critical information consists of specific facts about friendly Capabilities, Activities, Limitations (includes vulnerabilities), and Intentions (CALI) needed by adversaries for them to plan and act effectively to degrade friendly mission accomplishment.

(3) Critical information is information vital to a mission. If an adversary obtains it, correctly analyzes it, and acts upon it, the compromise could prevent or seriously degrade mission success. The goal is to deny our adversaries access to any critical information.

(4) Critical information is primarily unclassified, but can be classified depending on the organization, activity, or mission. Critical information that is classified requires OPSEC measures for additional protection because unclassified indicators can reveal it. Critical information that is unclassified especially requires OPSEC measures because it is not protected by the requirements provided to classified information.

c. Critical Information List (CIL) Is a consolidated list of a unit or organization's critical information. Every organization's OPSEC Officer must create a CIL specific for their organization In Accordance With (IAW) Army Regulation (AR) OPSEC (AR 530-1). The III Corps and Fort Hood CIL is provided in Appendix C.

d. Sensitive Information and Controlled Unclassified Information (CUI) requires protection from disclosure that could cause a compromise or constitute a threat to national security, an Army organization, activity, Family Member, Department of the Army (DA) Civilian, or DoD contractor. See DOD Manual 5200.01, Volume 4.

e. OPSEC Compromise

(1) An OPSEC compromise is the disclosure of S/CI that jeopardizes the unit's ability to execute its mission or to protect its personnel and/or equipment or effects national security.

(2) For S/CI that has been compromised and is available in open sources, the public domain should not be highlighted or referenced publicly outside of intra-governmental or authorized official communications, because these actions provide further unnecessary exposure of the compromised information. Personnel should not respond to queries to deny or confirm the validity of sensitive information that has been compromised or released to the public. Notify your organization's OPSEC officer and security manager of all OPSEC compromises.

1-6. Requirement

a. The National OPSEC Program, enacted by President Ronald Reagan in 1988, is outlined in National Security Decision Directive 298 (NSDD 298) and requires that each executive department and agency with a national security mission must have an OPSEC program. DoDD 5205.02E, supports the national program and requires each DOD component to have an OPSEC program. AR 530-1 requires that all units at battalion level or higher echelon (Commander or Director is a Lieutenant Colonel or Civilian equivalent) and above must have an active OPSEC program. This applies to any unit or activity authorized by a Modified Table of Organization and Equipment (MTOE) or a Table of Distribution and Allowances (TDA).

b. OPSEC maintains essential secrecy, which is the condition achieved by the denial of critical information to adversaries. Adversaries in possession of critical information can hinder or prevent friendly mission accomplishment. Thus, essential secrecy is a prerequisite for effective operations. Essential secrecy depends on the combination and full implementation of two approaches to protection:

(1) OPSEC denies adversaries critical information and indicators of sensitive information.

(2) Traditional security programs that deny adversaries classified, sensitive, and/or critical information are as follows:

(a) Information Security (INFOSEC)
(b) Information Assurance (IA)
(c) Electronic Security (ELSEC)
(d) Emission Security (EMSEC)
(e) Military Deception (MILDEC)
(f). Physical Security
(g) Force Protection (FP)
(h) Program Protection Planning
(i) Personnel Security (PERSEC)
(j) Industrial Security

c. OPSEC provides a methodology to manage risk. It is impossible to avoid all risk and protect everything. To attempt complete protection, necessary resources would have to be diverted from actions required for mission accomplishment.

1-7. Application

a. OPSEC awareness and execution is crucial to Army success. OPSEC is applicable to all missions and supporting activities on a daily basis. OPSEC denies adversaries information about friendly CALI that adversary leaders need in order to

make decisions to act against the U.S. or prevent friendly mission accomplishment. OPSEC applies to all Army activities and is required during training, sustaining, mobilizing, preparing for, and conducting operations, exercises, tests, or activities.

(1) OPSEC contributes directly to the Army's ability to employ forces and gain superiority over an adversary across the full spectrum of operations. Without S/CI about our forces, adversaries cannot effectively design and build systems, devise tactics, train, or otherwise prepare their forces (physically or psychologically) in time to effectively counter the Army's CALI, and exploit the Army's limitations.

(2) Combat capability increasingly depends upon gaining and maintaining information superiority and affects all aspects of raising, equipping, training, deploying, employing, and sustaining forces. Every Army organization produces or has information that ultimately affects the ability of U.S. forces to accomplish missions. Every organization must identify and protect this information (e.g., emerging Tactics, Techniques, and Procedures (TTPs)) that an adversary could use against U.S. forces.

(3) Research, Development, Test, and Evaluation (RDT&E) activities are particularly vulnerable to sensitive information and technology disclosure, both classified and unclassified, due to the long life of the development process; large number of personnel, organizations, and contracted companies involved. S/CI lost during the development process can result in an adversary countermeasure being developed even before a system is fielded. Systems protection, to include the acquisition process, is necessary to preserve the advantage of technological superiority of U.S. forces. OPSEC assessments and surveys will be used to evaluate the vulnerabilities of sensitive information and technology during the RDT&E phases

(4) Army Program Executive Officers (PEOs), program, project, or product managers, and contracting officials must consider OPSEC as a stipulation in all contracts. All requirements packages must receive two OPSEC reviews by the Requiring Activity (RA) OPSEC officer.

(a) At the beginning of the contracting process to determine if OPSEC requirements are needed in the Performance Work Statement (PWS).

(b) At the end of the contracting process for sensitive and/or critical information prior to public release. For additional guidance, see paragraph 2–7 and chapter 6 of this regulation.

b. OPSEC is more important now than it has ever been. The U.S. faces cunning and ruthless adversaries using asymmetric techniques to avoid our strengths. The first step for them to inflict harm is to gather information about us. They are exploiting the openness and freedoms of our society by aggressively reading and collecting material that is needlessly exposed to them. Good OPSEC practices can prevent these compromises and allow us to maintain essential secrecy regarding our operations.

1-8. Proponent

The Deputy Chief of Staff (DCS) G-3/5/7 is the Army's proponent for OPSEC. Subsequently, the staff proponency for OPSEC is the operations section. In organizations without a specified operations staff, the element with primary responsibility for planning, coordinating, and executing the organization's mission activities will be the proponent for OPSEC.

a. Although OPSEC is an operations function, it requires close integration with other security programs. While OPSEC is not an intelligence function, it relies heavily upon intelligence processes for threat development and an effective program evaluation.

b. A unit or organization's commander, operations officer, and the OPSEC Officer must incorporate OPSEC in all unit activities to maintain operational effectiveness.

(1) Unit actions are a primary source of indicators collected by adversaries. The commander, advised by the OPSEC Officer, controls these actions, assigns tasks, and allocates resources to implement OPSEC measures (see Appendix F).

(2) By observing activities, the OPSEC Officer can evaluate these measures for their effectiveness and their impact on operational success.

c. While the OPSEC Officer is responsible for the development, organization, and administration of an effective OPSEC program, commander's emphasis and support is essential to ensure the proper implementation of an OPSEC program.

Chapter 2
Responsibilities

2-1. All Personnel

OPSEC is everyone's responsibility. However, the success or failure of OPSEC is ultimately the responsibility of the commander and most important emphasis for implementing OPSEC comes from the chain of command. Failure to implement OPSEC measures properly can result in serious injury or death to our personnel, damage to weapons systems, equipment and facilities, loss of sensitive technologies, and mission failure. OPSEC is a continuous process and an inherent part of military culture and as such, must be fully integrated into the execution of all Army operations and supporting activities. All personnel, active component and reserve component, to include civilians and contractors supporting the military, will:

a. Know what their organization considers S/CI, where it is located, who is responsible for it, how to protect it, and why it needs to be protected.

b. Protect from unauthorized disclosure any S/CI to which they have personal access to including from other branches of service, contractor proprietary information, and foreign governments.

(1) Commanders will issue orders, directives, and policies for unit or organization personnel to protect S/CI. As well as clearly define the specific OPSEC measures all personnel will practice.

(2) A 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), other disciplinary, administrative, or other actions as applicable.

(3) Personnel not subject to the UCMJ who fail to protect S/CI from unauthorized disclosure may be subject to administrative, disciplinary, contractual, and/or criminal action.

c. Prevent unauthorized disclosure of S/CI.

d. Actively encourage others (including Family Members and Family Readiness Groups (FRGs)) to protect sensitive and/or critical information.

e. Know who their unit, activity, or installation OPSEC Program Manager (PM)/officer is, and contact them for questions, concerns, or recommendations for OPSEC-related topics.

f. Comply with command policy/direction as well as existing regulations prior to publishing or posting sensitive and/ or critical information that may be released into the public domain.

(1) This includes all voice, text, technical data communications, and other emerging Internet-Based Capabilities (IBC).

(2) Each unit or organization's OPSEC officer will advise supervisors on means to prevent the disclosure of sensitive and/or critical information. Supervisors will advise personnel to ensure that sensitive and/or critical information is not disclosed.

g. Handle attempts by unauthorized personnel to solicit sensitive and/or critical information as a Threat Awareness and Reporting Program incident per AR 381–12.

h. Destroy (burn, shred, and so forth) sensitive and/or critical information that is no longer needed to prevent the inadvertent disclosure and reconstruction of this material per applicable standards; see AR 380–5 (Department of the Army Information Security Program), for further guidance.

2-2. Commanders at All Levels

a. Commanders at all levels are responsible for ensuring their units or activities plan, integrate, and implement OPSEC measures to protect their command's S/CI in every phase of all operations, exercises, tests, or activities.

b. Commanders at all levels, or their official designees, are responsible for issuing signed orders, directives, and policies to protect their command's S/CI which will clearly define the specific OPSEC measures their personnel will practice.

c. Commanders will ensure their OPSEC program or OPSEC measures are coordinated and synchronized with the supported and supporting higher command's OPSEC Program and security programs such as INFOSEC, IA, physical security, and FP.

d. Commanders will ensure all official information released to the public domain receives an OPSEC review by an Headquarters, Department of the Army (HQDA) OPSEC Officer Level II trained OPSEC Officer prior to dissemination. The OPSEC review will not be conducted by the individual who originated the material to be released.

e. Commanders will ensure all OPSEC program documents are reviewed annually to ensure any changes in mission, threat, CIL or OPSEC measures are updated into the plan in a timely manner. Annual reviews should also assess if adequate resources are on hand to establish and maintain a successful program, if OPSEC Support Elements are being utilized, their effectiveness, and if education, training, and awareness is being conducted throughout the workforce. A memorandum attached to an OPSEC document that is more than a year old can be used to verify that the document was reviewed and if there were any changes.

2-3. Commanders of Units, Activities, Directorates at Battalion, and Higher Echelons, 2-3

Note. For the purpose of this regulation, a unit or activity is at battalion level or a higher echelon when its commander or director is a Lieutenant Colonel (or Civilian equivalent) or higher. This applies to any unit or activity authorized by a MTOE or a TDA.

a. In addition to the requirements outlined in paragraph 2-2, commanders at battalion and higher echelons will develop and implement a functioning, active, and documented (formal) OPSEC program for their unit, activity, or directorate to meet their specific needs and to support the OPSEC programs of higher echelons. To develop and implement a formal OPSEC program, commanders will:

(1) Establish OPSEC as a command emphasized item and include OPSEC effectiveness as an evaluation objective for all operations, exercises, and activities.

(2) Appoint a primary and alternate OPSEC Officer, in writing, with responsibility for supervising the execution of the OPSEC program within the organization.

(3) Ensure the appointed OPSEC Officers receive appropriate training IAW Chapter 4 of this regulation and they are of sufficient rank/ grade to execute their responsibilities.

(4) Establish a documented OPSEC program that as a minimum includes OPSEC Officer appointment orders and OPSEC documents. OPSEC documents shall include the unit or activity's threat assessment in writing, CIL, vulnerability assessment, risk assessment, and OPSEC measures to protect critical information.

(5) If assigned intelligence/counterintelligence capabilities, provide intelligence, and counterintelligence support to the command's OPSEC program. When this is not practical or possible, forward requirements to the next higher OPSEC Officer. The OPSEC process depends on reliable intelligence/counterintelligence support to properly identify critical information, analyze the threat, analyze vulnerabilities, conduct a risk assessment, and implement OPSEC measures.

(6) Approve the unit, activity, or directorate CIL. (The OPSEC Officer will develop and propose the CIL to the commander for approval.)

(a) Ensure all personnel know the unit, activity, and/or directorate critical information, and how to protect it.

(b) Provide guidance, direction to ensure each subordinate organization understands, adapts, applies the CIL to that organization's mission, and provides feedback to the commander.

(7) Conduct a risk assessment to determine what OPSEC measures are necessary and how they affect the mission. Then decide what OPSEC measures to implement.

(8) Publish OPSEC measures that must be practiced on a consistent basis that is specific to an operation, exercise, activity in Operation Plans (OPLANs), Operation Orders (OPORD), or in an OPSEC-directive.

(9) Ensure the OPSEC program addresses all personnel with access to S/CI (e.g. Soldiers, Civilians, Contractors, Family Members, and all other individuals who have access).

(10) Ensure OPSEC is incorporated and emphasized to the Family Readiness Support Assistant (FRSA) and FRG. This emphasis shall not be limited to periods of deployment or mobilization.

(11) Ensure OPSEC is incorporated into all contractual requirements and contracts that are both classified and unclassified involving S/CI (See chap 6).

(12) Provide appointed OPSEC Program Manager/Officer with opportunities to attend at other OPSEC-related courses, conferences, and meetings.

(13) Ensure the Public Affairs (PA) review process includes coordination with the OPSEC Officer IAW the command OPSEC document(s) to prevent the release of S/CI, which includes U.S. information that is determined to be exempt from public disclosure according to DODD 5230.09 (Clearance of DoD Information for Public Release), DODD 5230.25 (Withholding of Unclassified Technical Data from Public Disclosures) and DODD 5400.07 (Freedom of Information Act Program) or that is subjected to export controls according to International Traffic in Arms Regulation (ITAR), Export Administration Regulations (EAR), 15 CFR 768.1 et seq (Foreign Availability Determination Procedures and Criteria), AR 360–1 (Army Public Affairs Program), AR 70–14 (Army Safety Guide), AR 25–30 (The Army Publishing Program), and AR 380–5, and this regulation. A public affairs-qualified Non-Commisioned Officer (NCO) / Department of the Army (DA) Civilian / Officer may conduct this review. If unsure the information is releasable, the Public Affairs Officer (PAO) should consult the OPSEC officer of the owner of the information.

(14) The popularity and availability of a variety of Internet-based services (Social Networking Sites (SNS), photo sharing, blogs, etc.) has greatly increased the risk of inadvertent disclosures of S/CI and possibly classified information (alone or through compilation). These capabilities can be accessed from an ever-increasing number of mobile devices in addition to the traditional desktop workstation causing the reduction of reaction time and increases the risk to S/CI loss. This threat can be mitigated through OPSEC awareness training and guidance for those using these IBC. Commanders will ensure all OPSEC Program Managers, Officers and/or a coordinators, Information Operations (IO) professionals, PAO, FOIA Officers, contracting specialists, and personnel responsible for the review and approval of information intended for public release receive OPSEC training tailored to their duties.

(a) The designated reviewer(s) will conduct routine reviews of websites on a quarterly basis to ensure each website complies with the policies of AR 25-1 (Army Informational Technology) and the content remains relevant and appropriate. All OPSEC reviews will be documented.

(b) The minimum review will include all of the website management control checklist items in AR 25-1, Appendix C, paragraph C-4e(32-34). Information contained on publicly accessible websites is subject to the policies and clearance procedures prescribed in AR 360-1 (Army Public Affairs Program), Chapter 5, for the release of information to the public.

(c) Commanders will ensure their organizations using the Internet will not make S/CI available on publicly accessible websites.

b. Commanders may mandate that subordinate commands below battalion level develop and implement a formal OPSEC program, especially if these units have unique, highly visible, or highly sensitive missions.

c. Commanders may decide to incorporate subordinate commands into a higher echelon OPSEC program (for example, a battalion can incorporate its organic companies into its OPSEC program).

(1) This decision can apply to units with small force structures that are not commensurate with their designation (for example, units designated as a battalion but with a force structure similar to a company-size unit).

(2) Commanders shall mandate their subordinate commands determine their critical information, develop OPSEC measures to protect their critical information, and provide this information to a higher echelon OPSEC program.

d. Submit annual OPSEC report to higher headquarters.

2-4. The Garrison Commander

a. Responsible for issuing orders, directives, and policies to protect the command's S/CI and define the specific OPSEC measures that all personnel should practice.

b. Ensures that the command's OPSEC program and OPSEC measures are coordinated and synchronized with the higher command's security programs such as INFOSEC, IA, physical security, FP, and so forth.

c. Ensures all command official information released to the public receives an OPSEC review prior to dissemination.

d. Establishes a formal documented OPSEC program that includes at a minimum:

(1) An appointed OPSEC PM and alternate in writing with responsibility for the execution of the OPSEC Program on the installation.

(2) Both the appointed OPSEC PM and alternate must receive appropriate training IAW AR 530-1 chapter 4-2.

e. Develops an installation-level OPSEC Working Group (OWG) to coordinate OPSEC actions among the subordinate organizations and facilitate OPSEC guidance to them. An installation-level OWG can include, but is not limited to, tenant organization OPSEC officers, PAO, security managers, Antiterrorism (AT)/FP officers, Provost Marshal Office (PMO), Network Enterprise Center (NEC), and so forth.

f. Approves the organization's CIL and circulates the list 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 that organization's mission and provides feedback to the commander.

g. Consolidates and coordinates critical information from all tenant organizations to assist with the protection of the other tenant organizations' S/CI.

h. Weighs the risk in the mission against the costs of protection and decides what OPSEC measures to implement. Publish such measures in OPLANs and OPORDs.

i. Incorporates OPSEC into installation training and exercises and encourages tenant organizations to practice OPSEC measures in a garrison environment.

j. Provides annual reminders of the importance of sound OPSEC practices for the Fort Hood Sentinel.

2-5. Fort Hood OPSEC Program Manager

a. Serves as the Garrison Commander's principal staff officer for overall management of the Fort Hood OPSEC Program. The DPTMS is the proponent for OPSEC, but the entire staff must integrate OPSEC into planning and execution of the organization's activities.

b. Ensures the integration and synchronization of Fort Hood's OPSEC Program with Higher Headquarters (HHQ) OPSEC program.

c. Plans for and implements OPSEC before, during, and after operations and other activities that affect the combat capability of the U.S. Army. OPSEC is part of the commander's initial planning guidance.

d. Chairs the installation-level OWG. At Garrison level, the OPSEC manager develops an installation-level OWG to coordinate OPSEC actions among the tenant organizations and to facilitate OPSEC guidance to them. The OWG has been integrated into the Protection Working Group (PWG) IAW Installation Management Command (IMCOM) Installation Emergency Management Program (IEMP) Implementation (IMCOM FRAGO 001 to OPORD 10-094). The PWG is conducted the second Thursday of each month at 1000 in W217, III Corps Headquarters.

e. In conjunction with other staff officers input, develops the organization's CIL.

f. Develops and recommends OPSEC measures to be implemented within the Command.

g. Conducts OPSEC reviews of operational plans and reports to ensure adherence to OPSEC policies and procedures.

h. Conducts OPSEC assessments of subordinate units using the published OPSEC guidance to determine if the unit being assessed is implementing HHQ directed and their own OPSEC policies and procedures. The OPSEC officer submits a written assessment with results and recommendations to the assessed unit commander, or commander that directed the assessment.

i. Ensures training exercises include realistic OPSEC considerations and any evaluation of a training exercise includes an evaluation of OPSEC procedures. Further, ensure pre-exercise OPSEC briefings are conducted incorporating the threat, CIL, and OPSEC measures.

j. Promotes awareness and understanding of OPSEC, the OPSEC process, CIL, adversary intelligence threats, and individual responsibilities.

k. Coordinates OPSEC Level II training for the installation and serves as the primary Level III certified instructor.

l. Coordinates with the PA and FOIA officers to ensure an OPSEC review is conducted before the release of information concerning the command and/ or command programs and projects.

m. Ensures OPSEC training is conducted IAW AR 530-1 to include initial, pre-deployment, redeployment, External Official Presence (EOP), and FRGs.

n. Integrates intelligence, counterintelligence, FP, and IO into OPSEC planning and practice as appropriate.

o. Monitors the OPSEC programs of subordinate organizations by reviewing OPSEC Standard Operating Procedure (SOPs), survey results, exercise evaluations, and Inspector General (IG) reports.

p. Conducts an annual OPSEC assessment.

q. Prepares the annual OPSEC Program Report to be submitted to IMCOM region office.

r. Reviews and signs PWS for new contracts ensuring they include the AT/OPSEC Review Coversheet. The language of the contract must ensures proper adherence to OPSEC and annual OPSEC awareness training IAW Use of an Antiterrorism/Operations Security in Contracting Coversheet for Integrating AT/OPSEC into the Contract Support Process (ALARACT 015/2012)

s. Maintains contact with intelligence, law enforcement, and security agencies to obtain information that supports the OPSEC planning process.

t. Performs other duties and responsibilities as defined in AR 530-1, Appendix H.

2-6. Installation Support Directorates

a. Have an OPSEC program. An Army unit/activity at battalion level, higher echelon that has a commander, director at the Lieutenant Colonel level, Civilian equivalent, or higher requires an OPSEC Officer. This applies to any unit or activity authorized by a MTOE or a TDA.

b. Appoint a primary and alternate OPSEC Officer in writing with the responsibility for the execution of the OPSEC program within the organization.

c. Ensure the OPSEC Officers are properly trained.

d. Plan for and implement OPSEC before, during, and after operations and other activities that affect the capability of the Army. OPSEC is part of the commander's initial planning guidance.

e. Provide reminders of the importance of sound OPSEC practices. These reminders consist of OPSEC news releases in command publications, OPSEC information bulletins, OPSEC annual training, and OPSEC awareness briefings.

2-7. Installation Support Offices

OPSEC programs will be managed by the Plans, Analysis and Intergration Office (PAIO) OPSEC Officers (with the exception of the PAO) unless the director requests to maintain their own program.

2-8. The Public Affairs Office (PAO)

a. Appoint a primary and alternate OPSEC Officer in writing with the responsibility for the execution of the OPSEC Program within the organization.

b. 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 Web sites IAW AR 25-2 (Information Assurance), paragraph 4-20.g. (11).

c. Ensure that all Fort Hood personnel are aware of and support the Army's OPSEC program. The staff office or agency providing the information, materials, or records to the PAO for release should complete OPSEC reviews IAW AR 360-1, Chapter 5-4.

d. Consider OPSEC in all PA operations IAW Antiterrorism (AR 525-13), Appendix D-1.j

e. 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 personal safety, or invade the privacy of members of the Armed Forces, IAW AR 360-1, Chapter 2-3, paragraph d (5).

2-9. Organization Webmasters

a. Comply with Federal, DoD, and DA website administration policies and implement content-approval procedures that includes OPSEC and PAO reviews before updating or posting information on all websites IAW AR 25-2, Chapter 4-20, paragraph, g. (11).

b. Conduct annual OPSEC reviews of all organizational websites and include these results in their annual OPSEC reports pursuant to AR 530-1 and IAW AR 25-2, Chapter 4-2, paragraph, g (15).

c. Coordinate directly with the Command OPSEC Officer for additional guidance as needed on any questionable website postings.

d. Conduct annual EOP training.

2-10. Freedom of Information Act (FOIA) Officer

a. Release of information under the FOIA can have an adverse impact on OPSEC. FOIA and Privacy Act requests require automatic review by a qualified OPSEC Officer.

b. Coordinate with OPSEC PM to ensure the release of S/CI is not released.

c. The FOIA Officer for the staff agency or command will use DA Form 4948-R (Freedom of Information Act (FOIA)/Operations Security (OPSEC) Desk Top Guide) that lists references and information frequently used for FOIA requests related to OPSEC. The DA Persons who routinely deal with the public (by telephone or letter) on such requests should keep the form on their desks as a guide.

d. The FOIA Officer must ensure that no information is released to the public that is listed on the CIL.

e. The OPSEC review may require corrective action and an additional review.

f. OPSEC/FOIA advisors do not, by their actions, relieve FOIA personnel and custodians processing FOIA requests of their responsibility to protect classified or exempted information.

Chapter 3
Policy and Procedures

3-1. General.

OPSEC applies throughout the range of operations across the spectrum of conflict to all Army operations and supporting activities. The OPSEC program is a Commander's program (i.e. for all commanders and leaders) that consists of OPSEC planning, training, education and evaluation. It is designed so the units, staff, directorates, and all

personnel can practice OPSEC aggressively in order to deny adversaries critical information. OPSEC must be a post-wide effort that is integrated into all aspects of operations in order to increase the overall security posture. Therefore, leaders must create a positively enhanced environment for OPSEC to integrate its principles into the overall framework of INFOSEC, IA, physical security, and FP. All organizations at battalion-level and higher, including equivalent TDA organizations will have functional, active, and documented OPSEC programs. These programs will use the process described in this chapter to identify and protect critical information.

3-2. OPSEC Programs

A functional, active, and documented OPSEC program will have the following common features:

a. A primary and alternate OPSEC Officer appointed in writing.

(1) An OPSEC Officer is responsible for the development, organization, and administration of an OPSEC program at Division level and below. OPSEC PM are responsible for Corps and installation-level programs.

(2) While the OPSEC Officer is responsible for the development, organization, and administration of an OPSEC program, the commander's emphasis and support from the chain of command is essential to ensure the proper implementation of an OPSEC program.

(a) The appropriate rank/grade levels for OPSEC Officers are as follows:

1. Division: Captain (O-3) or above, Warrant Officer (CW2 or above), Noncommissioned Officer (E-8 or above), or GS-09.

2. Brigade: Captain (O-3) or above, Warrant Officer, Noncommissioned Officer (E-7 or above), or GS-09.

3. Battalion: First Lieutenant (O-2) or above, Warrant Officer, Noncommissioned Officer (E-6 or above) or GS-07.

(b) The Commander can approve, in writing (in the appointment memorandum /order), an exception to the rank/grade levels listed previously except for those below E-6.

(c) Organizations that do not employ a traditional military command structure will determine the appropriate rank/grade level for their OPSEC Officers.

(d) Contractors do not have authority over Soldiers and DA Civilians; therefore, contract employees will not be assigned as the command's OPSEC Officer. They may perform OPSEC duties in a supporting capacity.

(3) Primary and alternate OPSEC Officers will receive appropriate training for their duty positions (Chap 4).

b. An OPSEC program utilizes the five-step OPSEC process.

(1) The OPSEC process can apply to any plan, operation, program, project, or activity. It provides a framework for the systematic process necessary to identify and protect critical information. The process is continuous. It considers the changing nature of critical information, the threat, and vulnerability assessments throughout the operation. It uses the following steps:

(a) Identification of critical information - determine what information needs protection.

(b) Analysis of threats - identify the adversaries and how they can collect information.

(c) Analysis of vulnerabilities - analyze how the critical information might be exposed.

(d) Assessment of risk - assess the impact if the vulnerabilities are acted upon and what protective measures should be implemented to prevent that loss of information.

(e) Application of appropriate OPSEC measures that protect critical information.

(2) Refer to Appendix B for more details of the five-step OPSEC process.

c. OPSEC document(s), at a minimum, document the unit, activity, installation, or staff organization's critical information and OPSEC measures to protect it.

(1) OPSEC documentation will include command OPSEC policy, threat analysis, CIL indicators, a list of potential vulnerabilities and the associated risks, and OPSEC measures to mitigate the risks. The document can be in the form of an SOP, plan, or other procedural format.

(2) The unit or organization's CIL and OPSEC measures must be known by all assigned personnel in the organization.

(3) It is recommended to keep the number of items of critical information to fewer than 10 in order to aid in simplicity; however, the number of items on the CIL will be determined by the commander. In addition, the CIL must be disseminated or communicated to the lowest organizational level and personnel.

(4) Personnel must know the unit or organization's OPSEC measures and practice them on a consistent and continuous basis.

(5) OPSEC programs and documentation shall be reviewed at least annually to ensure any changes in mission, threat, CIL, or OPSEC measures are updated into the SOP/plan in a timely manner. A memorandum attached to an OPSEC document(s) more than a year old will be used to verify the SOP/plan has been reviewed and updated on an annual basis.

d. The OPSEC program must be coordinated and synchronized with the organization's other security programs such as INFOSEC, IA, physical security, and FP. Doing this will ensure the security programs do not provide conflicting guidance and support each other.

3-3. Program Awareness and Training Product Promotion

a. Active promotion of the OPSEC program is the responsibility of all levels of commands. Organizations are encouraged to develop their own OPSEC promotional materials, use all suitable techniques of publicity/promotion consistent with law, and funds available.

b. Appropriated funds may be used to buy items to promote the OPSEC program. Ideally, such items will be appropriate to the work environment or serve as a reminder of the benefits of participating in the program. Coffee mugs, key rings, lanyards, pens, tri-folds, posters, cards, etc. are typical promotional items.

c. As part of promotional efforts, commanders or directors at all levels should encourage the OPSEC Officer to:

(1) Advertise the OPSEC program with posters, billboards, inserts in bulletins, or other media, which frequently reaches Soldiers, DA Civilians, Contractors, and Family Members.

(2) Develop slogans, logos, and other materials designed to call attention to the OPSEC program.

3-4. Threat Analysis Support to OPSEC

The intelligence staff of the command will provide a written and up to date regional threat assessment in support of OPSEC. When this is not practical or possible, forward requirements through proper channels to the appropriate threat analysis center. The written threat information will be updated as necessary to reflect the organization's current situation and environment.

Chapter 4
Training Requirements

4-1. Overview

For OPSEC to be effective, all Army personnel (Soldiers, Civilian, and Contractors) must be aware of OPSEC and understand how the program complements traditional security programs. All personnel must know how to apply and practice OPSEC in the performance of their daily tasks. OPSEC must become a mindset of all Army personnel and be performed as second nature. To accomplish this level of OPSEC vigilance, OPSEC training programs must be action and job-oriented, enabling the workforce to put into practice the knowledge and TTPs they learned in training. Training should maximize the use of lessons learned to illustrate OPSEC objectives and requirements. In order to ensure accomplishment of training, commanders will include OPSEC training as a part of their organizations training guidance.

4-2. Training Levels

a. OPSEC Level I Training. The target audience for Level I is all personnel (Soldiers, Civilians, Contractors, and Family Members). Level I training is composed of both initial and continual awareness training:

(1) Initial OPSEC Awareness Training. All newly assigned personnel must receive initial training within the first 30 days of arrival to the organization. It is recommended this training be conducted as part of an initial entry briefing or unit/ organization newcomer's briefings. This training is provided by the unit or organization's OPSEC Officer and should be conducted face-to-face. The intent and focus of initial training will be on the following areas:

(a) Understanding the difference between OPSEC and other security programs and how OPSEC complements traditional security programs in order to maintain essential secrecy of U.S. military CALI and plans.

(b) Understanding what critical information is and how to protect it.

(c) How adversaries aggressively seek information on U.S. military CALI and plans.

(d) Specific guidance on how to protect critical information through OPSEC measures.

(e) End state: Each individual should have the requisite knowledge to safeguard critical information and know the answers to the following questions:

- What is my unit or organization's critical information?
- What critical information am I personally responsible for protecting?
- How is the threat trying to acquire my critical information?
- What steps am I/are we taking to protect my/our critical information?
- Who is my OPSEC Officer (in order to report an OPSEC compromise or ask an OPSEC question)?

(2) Continuous OPSEC Awareness Training. OPSEC awareness training must be continually provided to the workforce, reemphasizing the importance of sound OPSEC practices.

(a) This training consists of, but is not limited to, periodic OPSEC news releases in local command publications, OPSEC posters in unit areas, OPSEC information bulletins on unit bulletin boards and OPSEC awareness briefings by unit OPSEC Officers/Commanders.

(b) At a minimum, all Army personnel must also receive annual OPSEC awareness training provided by the unit or organization's OPSEC Officer or online. This training must be updated with current information, tailored for the unit's specific mission, and critical information.

(c) OPSEC training must be provided to deploying and redeploying units.

(d) OPSEC Officers will produce and make available OPSEC training for FRGs at meetings, commander’s call, and town hall meetings.

b. OPSEC Level II Training (HQDA OPSEC Officer’s Course). The target audience for Level II training is as follows:

(1) Primary and alternate OPSEC Officers are required to complete Level II training.

(2) OPSEC Coordinators, webmasters, PAOs, FOIA, FRSAs, or any other personnel who interact with the public on a regular basis are strongly recommended to attend the Level II Course.

(3) The HQDA OPSEC Officers Course will train and prepare personnel to manage an OPSEC program and advise the Commander in all OPSEC areas. Graduates will have the requisite knowledge in use of OPSEC analytic techniques. This training will allow the OPSEC Officer to identify vulnerabilities and select appropriate OPSEC measures. These acquired skills will assist the OPSEC Officer with planning, program development for overall program success, and mission effectiveness. They will also be qualified to provide the annual OPSEC Level I training.

(4) The Fort Hood OPSEC PM will host Level II training quarterly. These training courses are generally held the first week of November, February, May and August annually. In order to enroll into this course:

(a) Provide the Fort Hood OPSEC PM the following information: name, rank/grade, unit, phone number, email address, appointment orders, nomination form, and OPSEC 1301 (Fundamentals Course) training certificate.

(b) All attendees must have completed the Interagency OPSEC Support Staff (IOSS) OPSEC-1301 computer based training (E-learning). IOSS E-learning is completed by registration with IOSS at www.ioss.gov.

(c) All attendees must meet the eligibility requirements listed in Appendix H. Note**:** Walk-ins will not be allowed to train. Space is limited and many require this training. If an individual registers and does not attend without letting the aforementioned PM know prior to the start time, he or she will not be able to attend training in the future without a waiver from the first 0-6 or equivalent in their command.

4-3. Additional Training

a. OPSEC 1301. The IOSS OPSEC Fundamental Course or 1301 is a computer-based training that serves as the prerequisite training required prior to the start of OPSEC Level II training. The training can be found at www.IOSS.gov.

b. OPSEC 1500 (Analysis and Public Release Decisions Course). The IOSS course is delivered computer based or in person and addresses OPSEC issues that should be considered when reviewing information for public release and public access. Lessons can be applied to preparing information for release in all forms of media (e.g., print, web postings, and public speeches). After completing this course, the student will be able to edit information to be posted, written, and spoken by applying OPSEC principles and achieve the originator's objective without compromising critical information. This course is taught at the unclassified level. This course is specifically designed for individuals involved in determining what information should be released to the public, such as PAO, webmasters, FOIA Officers, speechwriters, speakers, classification review personnel, and OPSEC Officers/coordinators. Prerequisite**:** **None**. However, OPSEC-1301 is recommended.

c. OPSE 2500 (Analysis and Program Management Course)**.** This course addresses the basic skills and knowledge needed to conduct an OPSEC risk analysis (apply the five steps) and to implement an OPSEC program. The student is afforded the opportunity to apply OPSEC tools and lessons through a variety of practical exercises and case studies. Upon completing this course, students will be able to apply the systems analysis methodology to their organizations and activities; identify sources of information and support materials for OPSEC practitioners; conduct an OPSEC analysis of their program, activity or operation; market an OPSEC program; develop an organizational OPSEC policy; and implement and manage an OPSEC program. This course is designed for individuals performing the role of OPSEC PM. This course is taught at the unclassified level. Prerequisite**:** OPSE-1301 or equivalent.

d. OPSEC 3500 (OPSEC and IBC Course). This course introduces OPSEC practitioners to common threats, vulnerabilities, and countermeasures associated with IBC. It will allow OPSEC practitioners to better assess the risk when considering IBC. Upon

completion, students should be able to understand OPSEC concerns raised by IBC; understand the differences in motivations, skills, activities of adversaries, and how they constitute a threat to IBC. Understand the risks inherent to public IBC, appropriate countermeasures required to reduce those risks; be familiar with functions, benefits, vulnerabilities of emerging IBC technologies; and understand best practices to defeat commonly used attack techniques. Prerequisite**:** OPSEC 1301 or OPSEC 1500.

e. While the Internet is a powerful tool to convey information quickly and efficiently, it can also provide adversaries a potent instrument to obtain, correlate, and evaluate an unprecedented volume of aggregate information regarding U.S. capabilities, activities, limitations, and intentions.

(1) All commanders will ensure those personnel who publish or input information on EOP sites receives OPSEC training. This will be PAO/OPSEC training specific to persons whose duties include operating or maintaining EOP sites. All Soldiers, DA Cvilians, and contractors who post or maintain information or documents on the public domain for official purposes are required to take this computer-based training.

(2) Per AR 25–1, OPSEC officers and PAOs are required to conduct quarterly reviews of publicly accessible and registered military and/or government Web sites to ensure the information available does not compromise OPSEC. OPSEC PMs/officers will conduct an OPSEC review, and the PAO will prepare information for release in all forms of media (for example, print, Web posting, and public speeches).

4-4. Joint and Interagency Training

a. Joint OPSEC Support Element (JOSE). Provides direct support to the Joint Staff, Combatant Commanders, and Joint Force Commanders through integration of OPSEC into operational plans, and exercises. By providing staff level program development, training, and survey/assessments when directed. See https://www.iad.gov/ioss/index.cfm.

b. IOSS. Supports the National OPSEC Program by providing tailored training, assisting in program development, producing multimedia products, presenting conferences for the defense, security, intelligence, research, development, acquisition, and public safety communities. Its mission is to help government organizations develop their own, self-sufficient OPSEC programs, in order to protect U.S. programs and activities. IOSS is recognized as the standard for government OPSEC programs and provides subject matter expertise to the DoD. IOSS offers a multitude of OPSEC training aids that are available to all OPSEC Officers. See https://www.iad.gov/ioss/index.cfm.

Chapter 5
OPSEC Review, Assessment, and Survey
Section I
OPSEC Review

5-1. General
The OPSEC review is a documented evaluation of information or visual product to ensure protection of S/CI. These products include, but not limited to memoranda, letters, emails, articles, academic papers, videos, briefings, contracts, news releases, technical documents, proposals, plans, orders, and responses to FOIA/Privacy Act requests. The OPSEC Officer will conduct an OPSEC review of products related to U.S. military operations, and other supporting programs, prior to release in the public domain or to EOP sites. An OPSEC review is normallyconducted in conjunction with a PA review for the release of official information to the public. An OPSEC review is unrelated to the annual program review. The results of the review must be in writing with justifications annotated based on existing Laws, Executive Orders, DoD Directives, Instructions, ARs, and the organization's CIL.

5-2. Procedures
a. All OPSEC SOPs will state which products automatically go to the OPSEC Officer for a review.

(1) An individual may request an OPSEC Officer review their product or a commander may direct a review.

(2) News releases, web content, and responses to FOIA/Privacy Act requests are examples of products that require automatic review by a qualified OPSEC Officer (See 2-11 of this regulation).

(3) The specifics about whom conducts the reviews and how the reviews are conducted need to be outlined on the organization's SOP.

b. The OPSEC review may require corrective action and an additional review.

(1) When a compromise is reported or uncovered, corrective action must be recommended to the appropriate official in writing.

(2) The OPSEC Officer will provide a written request to other areas of expertise for additional review before a review can be completed (e.g., intelligence, FP, Foreign Disclosure Officer (FDO), and FOIA).

c. Technical papers and reports must contain distribution statements according to AR 25-30 (The Army Publishing Program), AR 70-31 (Standards for Technical Reporting), DoD Directive 5230.24 (Distribution Statements on Technical Documents), DoD Directive 5230.25(Withholding of Unclassified Technical Data from Public Disclosure) . This includes contractors producing technical information for the U.S. government.

d. IAW AR 25-1 and AR 25-2, sensitive information may not be placed on a website that is accessible to the public.

(1) All official organizational websites must have an OPSEC website review to ensure no information (See AR 25-1, paragraph 6-7c(3) and (4) and AR 25-2,

paragraph 4-20g (11) and (15)) is posted to or contained on any publicly accessible website.

(2) The OPSEC website review is the responsibility of the webmaster/maintainer, in coordination with the OPSEC Officer, PAO, and other appropriate designees (to include, but not limited to security, intelligence, and legal counsel) (see Appendix I for Website Review Checklist).

(3) Information not authorized for release to the public on any website is not releasable in any other public forum. Official websites must comply with all applicable Army and DoD guidance and policies.

e. The unit commander-approved CIL, in addition to restrictions stated in paragraphs b, c, and d above, provides a basis for determining release ability.

Section II
OPSEC Assessment

5-3. General

The OPSEC assessment is an evaluation process conducted annually of an organization, operation, activity, exercise, or support function to determine if sufficient OPSEC measures are in place to protect critical information. An OPSEC program assessment may include self-assessments or program reviews by IG inspections or HHQ assessments that specifically address OPSEC. The OPSEC assessment thus determines the overall OPSEC posture and degree of compliance in regard to subordinate organizations with published OPSEC plans and programs. The OPSEC assessment team should be composed of the OPSEC Officer and section representatives and others from throughout the organization.

5-4. Procedures

a. Each OPSEC Officer will conduct a self-assessment to determine the effectiveness of OPSEC measures and as a minimum track the status of the following:

(1) Identification of the OPSEC Officer.

(2) Unit personnel's knowledge of critical information or publication of the CIL.

(3) Unit personnel's knowledge of the collection threat to the unit.

(4) OPSEC measures in place to protect identified critical information.

(5) The status of OPSEC training.

b. At each command level, the organization must conduct an OPSEC assessment of subordinate units using the published OPSEC guidance to determine if the unit being assessed is implementing HHQ directed and their own OPSEC policies and procedures. The command OPSEC Officer will submit a written assessment with results and recommendations to the assessed unit's commander. As a minimum, the aforementioned items will be assessed in paraghraph (5-4 a).

c. An OPSEC assessment performed by a command OPSEC Officer as a minimum will include the following:

(1) Items in paragrahp 5-4a above.

(2) A formal OPSEC checklist based on restrictions listed in existing laws, statutes, and regulations (e.g., paragraph 5-2b, c and d above and Appendix I in this

regulation) and other specific requirements that may pertain only to the assessed organizations.

(a) The HHQ must develop and publish the OPSEC checklist as part of the Command Inspection Program (CIP).

(b) This does not preclude OPSEC assessments from being conducted other than as part of the annual CIP.

Section III
OPSEC Survey

5-5. General

a. A survey is a formal assessment conducted by a team of experts that analyze the activities associated with a specific organization, operation, activity, exercise, or support function by employing the known collection capabilities of potential adversaries. This evaluation should focus on the agency's ability to protect critical information from adversary intelligence exploitation during planning, preparation, execution, and post-execution phases of any operation or program.

b. OPSEC surveys are personnel, resource, time-intensive and should only be conducted when deemed necessary by the commander. Extremely sensitive programs, activities, operations where the slightest compromise will result in mission failure and/or extreme damage to national security are rare examples of where an OPSEC survey may be conducted.

c. Activities that warrant OPSEC surveys include, but are not limited to RDT&E; acquisitions; treaty verification; nonproliferation protocols; international agreements; FP operations; Special Assess Programs (SAP); and activities that prepare, sustain, and employ U.S. Military Forces over the range of military operations.

5-6. Procedures

a. The objective is to identify OPSEC vulnerabilities in operations or activities, which an adversary could exploit to degrade friendly effectiveness or the element of surprise. The survey helps the commander evaluate OPSEC measures and take further action, if necessary to protect critical information.

b. The OPSEC survey attempts to reproduce the intelligence image that a specific operation projects. The survey differs from an adversary's collection effort, since it occurs within a limited timeframe, and normally does not use covert means. From that image, it identifies exploitable information sources. It verifies the existence of indicators by examining all of an organization's functions during planning, coordination, and execution of operations. The examination traces the chronological flow of information from start to finish for each function.

c. The OPSEC surveys vary according to the nature of the information, the adversary collection capability, and the environment. In combat, surveys identify weaknesses that can endanger ongoing and impending combat operations. In peacetime, surveys assist in correcting weaknesses that disclose information useful to adversaries in future conflict, or in compromising ongoing research and development programs.

d. A survey will not serve as an inspection of the effectiveness of a command's security program or adherence to security directives. Each survey is unique, as it reflects the operation or activity it analyzes. Nevertheless, there are common procedures, which subsequent paragraphs discuss.

(1) To encourage open dialogue, a survey team will not attribute data to its source. An accurate survey depends on cooperation by all personnel in surveyed organizations.

(2) Reports are not submitted to the unit's HHQ. As appropriate, the survey team can provide lessons learned without reference to specific units or individuals. Additionally, if the Army OPSEC Support Element (OSE) conducts the survey a report is provided to the requesting commander.

e. Surveys fall under two types.

(1) A command survey concentrates on events, which happen solely within the command. It uses the personnel resources of the command to conduct the survey.

(2) A formal survey includes supporting activities beyond the control of the operation that are the focus of the survey (it crosses organizational lines with prior coordination). The survey team includes members from both inside and outside the surveyed organization. A letter or message initiates the formal survey. It states the subject, team members, and dates of the survey. It can also list organizations, activities, and locations. Contact the Army OSE for more information.

Chapter 6
OPSEC Contract and Subcontract Requirements

6-1. Overview

Contractors for defense systems acquisition programs, as well as other types of Army contracts, will practice OPSEC to protect classified, critical, and sensitive information for government contracts. The RA and the government contracting activity imposing contractual OPSEC measures requirements accomplish this. The RA OPSEC officer is responsible for reviewing all contractual documents to determine what OPSEC measures are required to protect critical and/or sensitive information. The RA will integrate OPSEC measures into their contract documents and coordinate with the government contracting activity to include OPSEC measures in the solicitation package and resultant contract using the AT/OPSEC coversheet.

6-2. Policy and Procedures

a. Commanders will establish procedures to document the review of all contractual documents by using the AT/ OPSEC Desk Reference coversheet to indicate review by the unit/organization OPSEC officer. The RA OPSEC officer will be involved at the beginning of the contract support process, to include providing associated OPSEC reviews as needed. If the RA does not have an appointed OPSEC officer, the RA's higher headquarters OPSEC officer will provide the OPSEC review.

b. For unclassified contracts, the RA OPSEC officer will review contractual documents to determine if any specific OPSEC measures are required in a contract.

The RA OPSEC officer will integrate any needed OPSEC measures into the PWS, the Statement Of Work (SOW), or the Statement Of Objectives (SOO)in sufficient detail to ensure complete contractor understanding of the exact OPSEC measures required by the RA. The government contracting activity will integrate the OPSEC measures into the solicitation package and resultant contract, based on the RA's coordination using the AT/OPSEC Desk Reference cover sheet. If the contract is modified or given another option year, this review process will be repeated to ensure required OPSEC measures remain current and relevant throughout the lifecycle of the contract.

c. The RA OPSEC officer will also perform an OPSEC review to identify any critical and/or sensitive information associated with the contract and, if found, determine specific OPSEC measures required in the contract prior to submitting the contractual documents to the government contracting activity. The unit's published CIL and OPSEC measures will provide the basis for this review. The OPSEC officer will coordinate with the RA for document modifications to eliminate or minimize any discovered critical and/or sensitive information. If critical information is part of the contractual document(s) or the RA believes any identified sensitive information should not be removed because it maintains the integrity of the contract, the RA will ask the government contracting activity to release the contractual document(s) in an online secure environment with controlled access and to ensure the solicitation package does not contain any critical and/or sensitive information, but instead refers to the secure location where the full document(s) can be accessed by appropriate personnel.

d. For classified contracts, the RA OPSEC officer will coordinate with the RA's industrial security specialist. If the RA does not have an industrial security specialist, the RA will coordinate through their chain of command for an industrial security specialist or submit a request to an appropriate outside agency for industrial security support for completion of a DD Form 254 (Department of Defense Contract Security Classification Specification). The industrial security specialist completes the DD Form 254, which is used to convey security requirements in a classified contract. Contractor input is encouraged but is not required. The industrial security specialist will review the SOW, SOO, or PWS to ensure the appropriate security clauses and/or language are contained therein to address the protection of classified information. The industrial security specialist ensures the OPSEC measures contained in the SOW, SOO, or PWS are also reflected on the DD Form 254. The industrial security specialist will forward the fully executed DD Form 254 to the RA for submission to the government contracting activity. If the contract is modified or given another option year, this process will be repeated to ensure the DD Form 254 remains current and relevant throughout the lifecycle of the contract.

Chapter 7
Special Access Programs (SAP)

7-1. Overview

a. A SAP is a security program established under Executive Order (EO) 12356 (National Security Information) and authorized by the Secretary of Defense to administer extraordinary security measures to control access and provide protection of extremely sensitive information in addition to the provisions of AR 380-5 for classified information.

b. AR 380-381 (SAPS and Sensitive Activities) and the DoD Overprint to the National Industrial Security Program Operating Manual (NISPOM) Supplement prescribe policies, procedures for establishing, administratively controlling, supporting, and decertifying SAPs.

7-2. Policy

Each SAP will have a functioning OPSEC program with an appointed OPSEC Officer from conception to disestablishment. The OPSEC program will use the process described in chapter 3 to identify and protect critical information. It will have a written OPSEC plan or annex. Each SAP involved in acquisition systems will include an OPSEC plan as a part of the Program Protection Plan (PPP).

a. The DCS, G-3/5/7, in coordination with the DCS, G-2, and Technology Management Office will provide policy guidance and HQDA staff oversight for SAP OPSEC procedures.

b. According to AR 380-381, the SAP Program Security Manager serves as the program point of contact for all security, counterintelligence, and OPSEC-related issues. The SAP Program Security Manager may serve as the SAP OPSEC Officer in SAPs that have small personnel strengths. However, the SAP OPSEC Officer may be a separate appointment apart from the SAP Program Security Manager if staffing allows.

c. The SAP OPSEC Officer will comply with the provisions of Chapter 3 of this regulation and AR 380-381. The SAP OPSEC Officer will manage and document the SAP's OPSEC program. The SAP OPSEC Officer is the liaison between the SAP and the command for OPSEC issues. Due to stringent SAP security measures, the organization's OPSEC PM/Officer may not always have knowledge of the SAP.

APPENDIX A
References

Section I. Required Publications

ALARACT 015/2012
Use of an Antiterrorism/Operations Security (AT/OPSEC) in Contracting Cover Sheet for Integrating AT OPSEC into the Contract Support Process citied in para 2-5(r)

ALARACT 421/2011
Army Operations Security (OPSEC) Training for External Official Presences Sites (EOP) Operators cited in para 4-3e

AR 25-1
Army Information Technology citied in para 2-3(14a),2-3(14b), 5-2(d1), Appendix G-3(a)

AR 25-2
Information Assurance citied in para 2-8 (b), 2-9 (a), 2-9(b),2-10,5-2(d1), Appendix G-3(a), Appendix I

AR 25-30
The Army Publishing program citied in para 5-2(2-2c)

AR 25-55
The Department of the Army Freedom of Information Act Program citied in para 1-5(2c), Terms 1-5(2f)

AR 70-31
Standards for Technical Reporting citied in para 5-2(2-2c)

AR 340-21
The Army Privacy Program citied in para 1-5(2f), Terms

AR 360-1
Army Public Affairs Program citied in para 2-3(14b), 2-8(d), 2-8(e), Appendix I

AR 380-40
Safeguarding and Controlling Communication Security Material citied in Appendix G-3(c)

AR 380-5
Department of the Army Information Security Program citied in para 1-5(2), 2-1(h), 2-1(i), 7-1(a), Appendix G-2(b), Terms

AR 380-381
Special Access Programed (SAPS) and Sensistive Activities Activities citied in para 7-1(b), 7-2(b), 7-2(c), Terms

AR 381-12
Threat Awareness and Reporting Program citied in para 2-1(h)

AR 381-102
U.S. Army Cover Support Program (U) citied in Appendix B-4(3d)

AR 525-13
Antiterrorism citied in para 2-4(e), 2-5 (r), 2-8 (d), H-7 (5), Appendix H

AR 525-21
Army Military Deception (MILDEC) Program citied in para B-4(3d)

AR 530-1
Operations Security (OPSEC) citied in para 1-5(4C-1),1-5(2f),1-6, 2-4(2), 2-5(m), 2-5(t), 2-109b), 6-2(h4), Appendix I, Terms

Computer Security Act of 1987 [Public Law 100-235]

DA Form 4948-R
Freedom of Information Act (FOIA) / Operations Security (OPSEC) Desk Top Guide citied in para 2-10(c)

DD Form 254
Department of Defense Contract Security Classification Specification citied in para 6-2(c)

DI-MGMT-80934C
Data Item Description Operations Security (OPSEC) Plan citied in para 6-2(f)

DODD 5000.01
Defense AcquisitionSystem cited in Section II Terms, 2-3 (a13)

DODD 5205.02E
DoD Operations Security (OPSEC) Program citied in para 1-5(a1), 1-5(2f), 1-6

DODD 5230.09
Clearance of DoD Information for Public Release cited in para 2-3(a13)

DODD 5230.25
Withholding of Unclassified Technical Data from Public Disclosure cited in para 2-3(a13)

DODD 5400.07
DoD Freedom of Information Act (FOIA) Program citied in para 1-5(2f), Section II Terms

DoDI 5000.02
Operation of the Defense Acquisition System cited in para E4

DoDI 5200.39
Critical Program Information (CPI) Protection within Research Development, Test, and Evaluation (RDT &E) citied in paraSection II Terms, G9(a), G9(b)

DODM 5105.21v1
Sensitive Compartmented Information (SCI) Administrative Security Manual Administration of Information and Information System Security, citied in para G9(b)

DODM 5200.01 Volume 4
DoD Information Security Program: Controlled Unclassified Information (CUI) cited in para Section II Terms, 1.5(d)

EO 13526
Classified National Security sited in para Section II Terms

Executive Order 13222
Continuatuon of Export Control Regulations, sited in para B2 (5) (b)

Executive Order 12356
National Security Information citied in para 7-1

Executive Order 12958
Classified National Security Information cited in para Section II Terms, G2(a)

Executive Order 13292
Further amendment to EO 12958, as amended, Classified National Security Information, citied in para Section II Terms, G2(a)

Export Administration Act of 1979 (50 USC App. 2401-2420) citied in para B2 (b5)

IMCOM FRAGO 01 to OPORD 10-094
Installation Emergency Management (IEM) Program Implementation citied in para 2-5

Joint Publication 2-0
Joint Intelligence citied in Appendix E-3

National Security Division Directive 298
National Operations Security (OPSEC) Program citied in para 1-6

Section II. Related Publications

Manchester Document, 2000
Citied in Appendix E-1(c)

OPSEC 1301
Fundemental Course Training Certificate citied in para 4-3 (b)

OPSEC 1500
Analysis and Public Release Decisions Course citied in para 4-3 (c)

OPSEC 2500
Analysis and Program Management Course

UCMJ, Article 92
Failure to obey order or regulation citied in para 2-1(2)
50 USC App. 2401-2420 (The Export Administration Act (EAA) of 1979) citied in para E4

EO 13222 (Continuation of Export Control Regulations) cited in para E4

APPENDIX B
The OPSEC Process

B-1. Overview
The OPSEC process consists of five steps that can apply to any plan, operation, program, project, or activity. These steps provide a framework for the systematic process necessary to identify, analyze, and protect sensitive information. The process is continuous and assessments should occur frequently throughout an operation. It considers the changing nature of critical information, the threat, and vulnerability assessments throughout the operation. It uses the following steps: identification of critical information; analysis of threats; analysis of vulnerabilities; assessment of risk; and application of OPSEC measures.

B-2. Identification of Critical Information
The purpose for this step is to determine what needs protection. This is one of the most difficult steps of the five-step process and is the most important to accomplish. OPSEC cannot protect everything, so the most important items should be afforded the greatest efforts of protection. The OPSEC Officer, in conjunction with input from other staff officers,' develops the unit or organization's critical information and provides it to the Commander, Director, or an individual in an equivalent position for approval.

a. Critical information consists of specific facts about friendly CALI. These facts are vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment.

(1) Critical information is information that is so vital to a mission that if an adversary obtains it, correctly analyzes it, and acts upon it, the compromise could prevent or seriously degrade mission success.

(2) Critical information can be classified or unclassified information, but is primarily unclassified. OPSEC measures protect the unclassified indicators that can reveal classified information.

(3) Critical information that is unclassified especially requires OPSEC measures because it is not protected by stringent well-defined requirements provided to classified information.

(4) Critical information can also be an action that provides an indicator of value to an adversary and places a friendly activity or operation at risk.

b. Several sources can help the OPSEC Officer determine the unit or organization's critical information.

(1) The supporting intelligence element will provide information on the adversary and its intelligence requirements.

(2) The next higher echelon publishes OPSEC guidance for subordinate units to support its OPSEC program. Subordinate units develop their critical information at the lowest level and forward their CIL to higher echelons. Higher echelons consolidate lower echelons critical information as a foundation for their own CIL. Final CILs from higher echelons are then sent down to subordinate units, which subordinate units must support.

(3) The Commander, Director, or equivalent leadership position will provide specific guidance.

(4) The Security Classification Guide (SCG) for a program or operation identifies classified critical information. The SCG itself identifies the most sensitive areas of an activity, program, project, or operation.

(5) Various laws and EOs require CUI to be protected. The following list contains examples of CUI but is not all-inclusive.

(a) Information concerning a protected person.

(b) Export controlled technical data (on the Military Critical Technologies List, as required by the Export Administration Act of 1979 (50 USC App. 2401-2420), extended by Executive Order 13222 under the International Emergency Economic Powers Act).

(c) Sensitive information (as defined in the Computer Security Act of 1987 (Public Law 100-235).

(d) Contract financial data in the pre-award stage.

(e) Military operational and tactical information.

(f) DoD-developed computer software.

(g) Proprietary data (trade secrets).

(h) Test materials used in an academic environment.

(i) Law Enforcement Sensitive information.

(j) Personally Identifiable Information (PII).

(6) Appendix C contains the Fort Hood CIL.

(7) Indicators that could reveal critical information are also considered critical information. Appendix D lists some samples of OPSEC indicators that could reveal critical information.

c. Identify the length of time critical information needs protection. Not all information needs protection for the duration of an operation.

d. The Commander must approve an organization's CIL and abide by critical information provided by HHQ.

e. The intent for the CIL is that all organization personnel (Soldiers, Civilians, and DoD contractors) be aware of the organization’s critical information so that they can apply OPSEC to their daily tasks. Characteristics of a good CIL include:

(a) Should be 10 items or less

(b) Be classified at the lowest possible level, preferably unclassified

(c) Be disseminated to the widest audience possible

(d) Should be simple and easy to remember

(3) Once the CIL has been created, OPSEC measures must be applied during operations, missions, training, war-gaming exercises, or other activities where that information might be compromised. The OPSEC officer will determine the period during which each critical element needs protection. Not all critical information needs to be protected throughout an operation. Some elements need to be protected only during specific events; others may need protection at all times. Examples of types of information that may be critical to an organization are below:

(a) Administration/Personnel

- Schedules revealing when sensitive events will occur.
- Orders and movement of units or key personnel.
- Trash and housekeeping functions revealing concealed sensitive activities.
- Casualty, damage, and serious incident reports.
- Lists identifying a lack of personnel in critical specialties.
- Rosters identifying personnel by position, military occupation specialty, rank, or social security number.
- Deployment manning documents related to troop movements.
- Detailed travel itineraries for high-risk personnel.
- Cancellation of leave or emergency recall of personnel.

(b) Intelligence

- Effectiveness and employment of collection platforms.
- Intelligence collection efforts and methods.
- Collection operations
- Human Intelligence (HUMINT) operations.
- Counter Intelligence (CI) operations.
- Threat Awareness Reporting Program (TARP) incidents.
- Foreign Intelligence Service (FIS) collection operations.

(c) Plans and Operations

- Operational readiness of units.
- Ongoing Future Operations Planning (FUOPS) or specialized training.
- Dates of deployment/redeployment.
- Ports of debarkation/embarkation.
- Publishing undisclosed mission of units.
- The location of future assignments for units.
- Planning, deployment, and operations in support of contingency operations.
- Emerging TTP.
- Photos of battle losses or ongoing operations.
- Information negatively affecting foreign relations with allies or world opinion.
- Equipment or security vulnerabilities.
- OPSEC vulnerabilities.
- Rules of engagement.
- Call signs and frequencies.

(d) Logistics

- Publishing undisclosed readiness reports or logistical shortfalls.
- Facts concerning unit receiving specialized equipment.

(e) Installation

- Location and types of weapons stored.
- Sensitive projects or units.

- Critical storage facilities.
- Critical infrastructure and vulnerabilities.

B-3. Analysis of Threats

a. The purpose of this step is to identify adversary collection capabilities against critical information. Adversary collection activities target actions and open source information to obtain and exploit indicators that will negatively affect the mission. OPSEC indicators are friendly detectable actions and open source information that can be interpreted or pieced together by an adversary to derive critical information (See Appendix D for sample OPSEC indicators).

b. Methodology.

(1) In coordination with the intelligence staff and all other staff elements, examine each part of the activity or operation to find actions or information that will provide indicators in each area (personnel, logistics, communications, movement activities, aviation, etc.).

(2) Compare the identified indicators with the adversary's intelligence collection capabilities. A vulnerability exists when the adversary can collect an indicator of critical information, correctly analyze the information, make a decision, and take timely action to adversely influence, degrade, or prevent friendly operations. One method to use is to develop a "mission timeline." Identify along the timeline anything the commander has stated that he or she wants protected.

(3) Have each staff element or participant in the action/operation to identify along the "timeline" actions that "must be accomplished" in order for the mission to be accomplished.

(4) Identify which of these "must be accomplished" actions will be indicators an adversary could use. Now compare each indicator with each of the adversary's collection capabilities. Where there is a match, there is a vulnerability. Consider the following questions:

(a) What critical information does the adversary already know? Is it too late to protect information already known by an adversary?

(b) What OPSEC indicators will friendly activities create about the critical information not already known by the adversary?

(c) What indicators can the adversary actually collect? (This depends on the capabilities of the adversary's intelligence system.)

(d) What indicators will the adversary be able to use against friendly forces?

(e) Which indicators can be used to friendly advantage by fostering a desired perception by the adversary that will be beneficial to friendly operations? (Coordinate with MILDEC planners and Military Information Support Operations (MISO Officers.)

B-4. Analysis of Vulnerabilities

The purpose of this step is to identify each vulnerability and draft tentative OPSEC measures addressing those vulnerabilities. The most desirable measures provide needed protection at the least amount of cost to operational effectiveness and efficiency.

a. OPSEC measures are methods and means to gain and maintain essential secrecy about critical information. There are three categories of measures to accomplish this.

(1) Action control consists of measures to control friendly activities. Action control can eliminate or reduce indicators or the vulnerability of actions to exploitation by adversary intelligence systems to an acceptable level. Select what actions to undertake, decide whether or not to execute actions or impose restraints on actions (trash control, mandatory use of secure communications, OPSEC reviews, etc.). Specify who, when, where and how.

(2) Countermeasures disrupt the adversary's information gathering or prevent their recognition of indicators when collected materials are processed. Use diversions, camouflage, concealment, jamming, deterrence, police powers, and force against adversary information gathering and processing capabilities.

(3) Counter analysis is directed at the adversary analyst to prevent accurate interpretations of indicators during adversary analysis of collected material. Confuse the adversary analyst through deception techniques such as cover.

b. Select at least one tentative OPSEC measure for each identified vulnerability. Some measures may apply to more than one vulnerability. Specify who, when, where, how and for how long the measure is to be in effect.

c. Assess the sufficiency of routine security measures (personnel, physical, cryptographic, document, special access, automated information systems, and so on). These will provide OPSEC measures for some vulnerabilities.

d. If required, refer to AR 525-21 (Army Military Deception (MILDEC) Program (U) (C)) for information on deception and refer to AR 381-102 (U.S. Army Cover Program (S)) for information on cover.

e. Appendix F has sample OPSEC measures.

B-5. Assessment of Risk

In OPSEC, a risk can be defined as the probability an adversary will compromise critical information and the impact if the adversary is successful. Not all risks can be avoided without the loss of mission effectiveness or efficiency; therefore, the risks have to be managed to an acceptable level. The purpose of this step is for the OPSEC Officer to select which of the tentative OPSEC measures to implement and recommend them to the commander. The commander responsible for the mission must make the final decision and balance the risk of operational failure against the cost of OPSEC measures.

a. Consider the following questions for each tentative measure. The OPSEC Officer must be prepared to answer each of these questions for the Commander.

(1) What is the likely impact of an OPSEC measure on operational effectiveness if implemented?

(2) What is the probable risk to mission success (effectiveness) if the unit does not implement an OPSEC measure?

(3) What is the probable risk to mission success if an OPSEC measure does not work?

(4) What is the impact on future missions if this measure is adopted and successful?

(5) What is the impact to other units of practicing an OPSEC measure?

b. Decide which, if any, OPSEC measures to recommend for implementation and when to do so

. c. Check the interaction of OPSEC measures. Ensure that a measure to protect a specific piece of critical information does not unwittingly provide an indicator of another (e.g., radio blackout might indicate to collectors that a death may have occurred).

d. Determine the coordination requirements for OPSEC measures with the other capabilities (e.g., MILDEC).

e. Submit the final selected OPSEC measures to the commander for approval.

f. The commander may decide on a no-measures alternative. This is acceptable, if the OPSEC process was used to determine that no critical information requires protection or that the costs outweigh the risks. However, that decision must be documented for future reference.

B-6. Application of Appropriate OPSEC Measures

a. The purpose of this step is to apply OPSEC measures, approved by the commander, to ongoing activities or to incorporate them into plans for future operations.

(1) The OPSEC Officer implements OPSEC measures by generating guidance or tasking. The guidance or tasking can be in the form of annexes to plans, OPSEC plans, SOPs, and memoranda. The OPSEC Officer will:

(a) Incorporate OPSEC measures into the operation, activity, acquisition program, or project. Under the commander's authority, direct the implementation of those measures that require immediate action. This applies to current operations as well as planning and preparation for future ones.

(b) Document the OPSEC measures. Operations, exercises, RDT&E programs, acquisition programs, and other activities of interest to adversary intelligence services will have an OPSEC annex or plan (if the commander selected a no-measures alternative, ensure that is annotated).

(c) Brief OPSEC requirements to planners, participants, and support personnel. OPSEC measures are command-directed actions executed by individuals who must be aware of their responsibilities. Emphasize the adverse results of a failure to maintain effective OPSEC, particularly for long-term undertakings such as RDT&E programs.

(2) Personnel within the organization execute OPSEC measures. The role unit personnel play begins upon receipt of the OPSEC guidance or tasking. By complying with the published OPSEC guidance or tasking, unit personnel functionally implement the required OPSEC measures.

b. After the implementation of appropriate measures, the OPSEC Officer should evaluate the effectiveness of OPSEC measures during execution.

(1) The application of OPSEC measures is a continuous cycle that includes evaluating intelligence and counterintelligence reports, public media disclosures, website reviews, integrated systems security monitoring, feedback on reports such as assessments and surveys.

(2) As part of the OPSEC evaluation process, OPSEC Officer will:

(a) Evaluate the effectiveness of current OPSEC measures.

(b) Provide emphasis when needed.

(c) Recommend adjustments to improve the effectiveness of existing measures.

(d) Recommend new measures if significant new vulnerabilities develop.

Table B-1:The Five-Part OPSEC Process Worksheet Sample

High (3) = 13-27 / Medium (2) = 4-12 / Low (1) = 1-3											
Step 1: Critical Information	Step 2: Threat			Step 3: Analyze Vulnerabilities		Step 4: Risk Assessment (R=T(VxI))				Step 5: Implement Measures	
CIL items	Type / Country	Rating	Method	Vulnerability / Indicators	Tentative Measures	T Rating (Constant)	V Rating	I Rating (Constant)	Risk (Total)	Measures	Residual Risk

B-7. Planning Guidance

a. OPSEC steps occur within the Military Decision Making Process (MDMP). The OPSEC Officer provides planning guidance for staff elements. Each staff element will identify the critical information, who is responsible for protecting it, and the vulnerabilities in their functional areas, and provide them to the OPSEC Officer.

b. OPSEC planning guidance (provided as an OPSEC estimate) includes the following items:

(1) An estimate of probable adversary knowledge of the activity or operation.

(2) A preliminary list of critical information.

(3) A summary of adversary intelligence collection capabilities.

(4) A list of OPSEC indicators by staff function.

(5) A list of OPSEC measures to implement immediately and additional measures to consider.

c. By incorporating OPSEC into planning early on, the activity or operation will be more effective during execution.

d. Example Situation. A unit may decide its upcoming deployment date is critical information. Critical information is revealed by visible indicators, for example the inoculations that often take place prior to deployment. These indicators can be detected by an adversary based on the assessed threat. Since virtually any adversary can observe a unit gathering for inoculations, the threat is legitimate in this case, and this is a vulnerability. To counter this vulnerability, the unit may direct an OPSEC measure,such as sending unit members in smaller groups for their inoculations. The OPSEC Officer would then observe and gauge the effectiveness of this measure and revise as appropriate.

APPENDIX C
Critical Information List

Operations Security protects sensitive, but generally unclassified information critical to our mission. Critical information consists of specific facts about our CALI. The critical information is so vital to the mission that if the adversary obtains it, correctly analyzes it, and acts upon it, the compromise could prevent or seriously degrade mission success. The CIL documents an organization's critical information that should be protected. The Fort Hood CIL is as follows:

- **S**ensitive Reports: reports containing sensitive and/or PII or information pertaining to mission readiness such as blotters, battle damage assessments, recall rosters, manning documents, etc.
- **E**merging TTP: newly administered TTPs to improve mission effectiveness such as ways to avoid or detect Improvised Explosive Devices (IED), convoy protection methods, etc.
- **N**etwork & Communications Related: call signs, frequencies, passwords, Automated Information Systems (AIS) protection (types used, measures, and procedures), changes in message volume, etc.
- **S**ecurity Plans and Procedures: Random Antiterrorism Measures, shift change for guards, changes in Force Protection Condition (FPCON), Defense Readiness Condition (DEFCON), or information Condition (INFOCON), etc.
- **I**ntelligence, Surveillance, and Reconnaissance (ISR): intelligence resources, collection techniques, ongoing operations and goals, counterintelligence operations, etc.
- **T**roop Movements & Travel: deployment/redeployment Date Time Group (DTG), locations, itineraries, ports, routes, embarkation points, Very Important Person (VIP)/High Risk Personnel (HRP) travel, Temporary Duty (TDY) orders, leave for large groups or entire units, emergency recall of personnel, etc.
- **I**nformation Pertaining to Current/ FUOPS: deployment plans, exercises, scope of operations, planning details, specific courses of action

(COA) for forces, Rules of Engagement (ROE) / Rules for the Use of Force (RUF), MISO and MILDEC operations, SAP elements in contracts, etc.
- **V**ulnerabilities: a condition that allows the adversary time to observe, orient, decide and act against us in areas such as critical infrastructure, building schematics that show security weaknesses, physical security shortfalls, etc.
- **E**quipment Specifications and Limitations: shortfalls, vehicle schematics, vehicle battle damage assessments, weapons systems, Research and Development (R&D) projects, electronic systems, software used in new systems, etc.

APPENDIX D
OPSEC Indicators

D-1 Overview

Indicators are data derived from open sources or from detectable actions that adversaries can piece together or interpret to reach personal conclusions or official estimates concerning friendly capabilities, activities, limitations, and intentions. An item which meets any of the characteristics below (signature, association, profile, contrast, or exposure) is an indicator. Indicators are the bits and pieces of information and data that the adversary analyst pieces together to develop his intelligence estimate. Indicators are what the adversary uses to formulate his perception of our operations. We can manage the adversary's perception by managing the indicators. OPSEC uses an adversary's perspective and modifies friendly profiles accordingly.

a. Signature. This characteristic makes an indicator identifiable or causes it to stand out. Uniqueness and stability are properties of a signature. Uncommon or unique features reduce the ambiguity of an indicator. An example is the unique design of the M–1-series main battle tank. Its visual signature cannot be mistaken from most tanks. A unique visual signature minimizes the number of other indicators that an adversary must observe to confirm its significance. An indicator's signature stability, which implies constant or stereotyped behavior, can allow an adversary to predict intentions. Varying the behavior decreases the signature's stability and thus increases the ambiguity of the adversary's observations. Procedural features are an important part of any indicator's signature and may provide the greatest value to an adversary. These features identify how, when, and where the indicator occurs and what part it plays in the overall scheme of operations and activities.

b. Associations. These are the keys to interpretation. Compare current with past information to identify possible relationships. Continuity of actions, objects, or other indicators, which register as patterns, provides another association. The presence of special operations aviation aircraft, such as the MH–6, MH–60, and MH–47, may be indicators of other SOF operating in the area. Certain items of equipment particular to specific units are indicators of the potential presence of related equipment. For example, the sighting of an M–88A2 Hercules Recovery Vehicle likely indicates the presence of an armored unit equipped with M1A2-series tanks, as the M–88A2 is rated to recover and tow the M1A2-series tanks. Such continuity can result from repetitive practices or sequencing instead of from planned procedures. When detecting some

components of symmetrically-arrayed organizations, the adversary can assume the existence of the rest. As another example, the adversary would suspect the presence of an entire infantry battalion, when intelligence detects the headquarters company and one line company. When taken as a whole, the pattern can be a single indicator, which simplifies the adversary's problem.

c. Profiles. Each functional activity has a profile made up of unique indicators, patterns, and associations. The profile of an aircraft deployment, for example, may be unique to the aircraft type or mission, as in the special operations aviation example. This profile, in turn, has several sub-profiles for the functional activities needed to deploy the particular mission aircraft (for example, fuels, avionics, munitions, communications, air traffic control, supply, personnel, and transportation). If a functional profile does not appear to change from one operation to the next, it is hard for an analyst to interpret. If, however, it is unique, it may contain the key or only indicator needed to understand the operation. Unique profiles cut the time needed to make accurate situation estimates. They are primary warning tools, because they provide a background for contrasts.

d. Contrasts. These are the most reliable means of detection, because they use changes in established profiles. They are simpler to use because they only need to be recognized, not understood. One question prompts several additional ones concerning contrasts in profile. The nature of the indicator's exposure is an important aspect when seeking profile contrasts. In the special operations aviation example, if the adversary identifies items unique to special operations aviation at an airfield, this will contrast with what is "normal" at the airfield and will indicate the deployment of special operations aircraft to the airfield without having actually observed them.

e. Exposure. Duration, repetition, and timing of an indicator's exposure affect its importance and meaning. Limited duration and repetition reduces detailed observation and associations. An indicator that appears over a long period of time becomes part of a profile. An indicator that appears for a short time will likely fade into the background of insignificant anomalies. Repetition is the most dangerous. Operations conducted the same way several times with little or no variation provide an adversary the information needed to determine where, when, how, and with what to attack. This is a lesson learned at the cost of many lives during every war.

D-2. Sample OPSEC Indicators

The following are examples of OPSEC indicators. Many indicators are possible for the wide range of Army operations and activities. The purpose of this appendix is to stimulate thinking. Do not use it as a checklist, since each operation or activity will have indicators unique to itself. This listing is not all inclusive, but merely provided to give OPSEC Officers an idea of some of the actions or information that can provide indication of what has happened, is happening, or is going to happen. Indicators must be viewed from the adversarial point of view. Think of the indicators as being pieces of a large puzzle, as the adversary collects each piece, the picture comes together. The adversary may not need every piece of the puzzle to get the overall picture of the mission or action.

D-3. Administration

a. TDY orders.
b. Conferences.
c. Transportation arrangements.
d. Billeting arrangements.
e. Medical care.
f. Schedules.
g. Plans of the day.
h. Leave for large groups or entire units.
i. Reserve mobilization.
j. Changes to daily schedules.
k. Change of mail addresses or arrangements to forward mail on a large scale.
l. Runs on Post Exchange for personal articles; for example, personal radios.
m. Emergency personnel requisitions and fills for critical skills.
n. Emergency recall of personnel on leave and pass.

D-4. Operations, Plans, and Training

a. Changes in DEFCON, FPCON, or INFOCON.
b. Movement of forces into position for operations.
c. Abnormal dispersions or concentrations of forces.
d. Deviations from routine training.
e. Rehearsals and drills for a particular mission.
f. Exercises and training in particular areas with particular forces.
g. Repeating operations the same way, same time, same route or in same area. Fixed schedules and routes.
h. Standard reactions to hostile acts.
i. Standardizing maneuvers or procedures.
j. Standardizing force mixes and numbers to execute particular missions down to squad level operations.
k. Changing guards at fixed times.
l. Appearance of special purpose units (bridge companies, pathfinders, Explosive Ordnance Detachments (EOD), special operations, Liaison Officer (LNO) teams, etc.).
m. Change in task organization or arrival of new attachments.
n. Artillery registration in new objective area.
o. Surge in food deliveries to planning staffs at major HQ.
p. Unit and equipment deployments from normal basis.

D-5. Communications

a. Voice and data (telephone, cellular phone, wireless) transmissions between participants in an operation.
b. Establishment of command nets.
c. Changes in message volume (phone calls to secure systems), such as increased radio, email, and telephone traffic from HQs.
d. Units reporting to new commanders.
e. Identification of units, tasks, or locations in unsecured transmissions.

f. Increased communications checks between units/organizations.
g. Unnecessary or unusual increase in reporting requirements.
h. Sudden imposition of communications security measures, such as radio silence.
i. Appearance of new radio stations in a net.
j. Communications exercises.
k. Appearance of different cryptographic equipment or materials.
l. Increase in unofficial use of commercial e-mail services.
m. Increased FRG/FRSA posture
n. Unofficial use of instant messenger and chat forums.

D-6. Intelligence, Counterintelligence, and Security

a. Concentrated reconnaissance in a particular area.
b. Embarking or moving special equipment.
c. Recruitment of personnel with particular language skills.
d. Routes of reconnaissance vehicles.
e. Sensor drops in target area.
f. Increased activity of friendly agent nets.
g. Increased ground patrols.
h. Unusual or increased requests for meteorological or oceanographic information.
i. Unique or highly visible security to load or guard special munitions or equipment.
j. Adversary radar, sonar, or visual detection of friendly units.
k. Trash and recycle bins that contain critical information.

D-7. Logistics

a. Volume and priority of requisitions.
b. Package or container labels that show the name of an operation, program, or unit designation.
c. Prepositioning equipment or supplies.
d. Procedural disparities in requisitioning and handling.
e. Accelerated maintenance of weapons and vehicles.
f. Presence of technical representatives.
g. Unusual equipment modification.
h. Increased motor pool activities.
i. Test equipment turnover.
j. Special equipment issue.
k. Stockpiling petroleum, oil, lubricants, and ammunition.
l. Upgraded Lines of Communication (LOCs).
m. Delivery of special or uncommon munitions.
n. New support contracts or host nation agreements.
o. Arranging for transportation and delivery support.
p. Requisitions in unusual quantities to be filled by a particular date.

D-8. Engineer

a. New facility leases.

b. Construction of mock-ups for special training.

c. Production or requisitions of unusual amounts of maps, charts, or products for unusual areas.

d. Attachment of specialized heavy equipment.

D-9. Medical

a. Stockpiling plasma and medical supplies.

b. Movement of deployable medical sets.

c. Immunization of units with area specific and time-dependent vaccines.

d. Identifying special medical personnel and teams deploying to specific areas.

e. Sudden recall of National Guard and Army Reserve doctors to active duty.

D-10. Emissions Other Than Communications

a. Radar and navigational aids that reveal location or identity.

b. Normal lighting in a blackout area.

c. Operating at unusual speed in water.

d. Loud vehicle or personnel movements.

e. Smoke and other odors.

D-11. Research, development, test and evaluation, and acquisition activities

a. Solicitations for subcontractors to perform portions of the work.

b. Lists of installations that are involved in particular contracts or projects.

c. Specialized hiring of personnel for particular contracts or projects.

d. Highlighting specific security needs or requirements for portions of a projector contract.

e. Testing range schedules.

f. Unencrypted emissions during tests and exercises.

g. Public media, particularly technical journals.

h. Budget data that provides insight into the objectives and scope of a system or the sustainability of a fielded system.

i. Deployment of unique units, targets, and sensor systems to support tests associated with particular equipment or systems.

j. Unusual or visible security imposed on particular development efforts that highlight their significance.

k. Special staffing for tests or assembly of personnel with special skills from manufacturers known to be working on a particular contract.

l. Stereotyped use of location, procedures, and sequences of actions when preparing for and executing test activity for specific types of equipment or systems.

m. Advertisements indicating that a company has a contract on a classified system or component of a system, possess technology of military significance, or have applied particular principles of physics and specific technologies to sensors and the guidance components of weapons.

n. Schedules (delivery, personnel arrival, transportation, test, ordnance loading, etc.) posted where personnel without a need-to-know have access.

o. Conferences, symposia, and internal professional forums

APPENDIX E
The Threat

E-1. Overview

a. Because the U.S. military is superior in traditional forms of warfare, adversaries and potential adversaries have shifted away from traditional warfare and have adopted asymmetric methods and means. In addition to traditional capabilities and methods, adversaries also will conduct irregular, catastrophic, and disruptive forms of warfare.

(1) Traditional threats are posed by adversaries employing recognized military capabilities and forces in familiar or symmetric forms of conflict.

(2) Irregular threats come from adversaries employing unconventional methods to counter the traditional advantages of stronger opponents.

(3) Catastrophic threats involve the acquisition, possession, and use of Weapons of Mass Destruction (WMD) or methods producing effects of WMD.

(4) Disruptive threats can come from adversaries who develop and use breakthrough technologies to negate U.S. advantages in key operational domains.

b. Adversaries are not limited to practicing one form of warfare and can be expected to gain and employ methods and capabilities from the other forms of warfare.

c. The asymmetric methods of warfare involve a strong emphasis on collecting information from unclassified and open sources. As a result of the U.S. is a free and open society, information is readily available and easy to access. Adversaries are exploiting this vulnerability by aggressively reading open source and unclassified material about the U.S. Army. As a result, many adversaries do not need to invest in costly and highly technical intelligence collection systems when they can obtain the information they are seeking openly and legally. The Manchester Metropolitan Police found what was later dubbed the Manchester Document. The document, linked to Osama bin Laden, was located in the home of an Al Qaeda operative who was operating in England. The handbook explains that 80% of information they collect comes from open sources.

E-2. Adversaries

a. Non-state actors. These adversaries do not have a formal and recognized government and are international or transnational in nature and as a result are difficult to identify and locate. They do not employ traditional military forces or intelligence services. They favor irregular warfare through terrorist tactics and methods but also seek disruptive and catastrophic means and methods. Non-state actors place an emphasis on collecting open source and unclassified information since they typically do not possess highly technical and expensive collection systems.

b. Nation-states. These adversaries are readily identifiable and employ traditional military forces and professional intelligence services that collect information through a variety of methods. They also place an emphasis on collecting open source and unclassified information as well as HUMINT collection since they are far less expensive and in some ways more effective than expensive and highly technical means of collection.

c. Domestic threats. Domestic adversaries are not as easily identifiable since they are part of the local population. They do not likely have a formal intelligence collection service but have the advantage of detailed knowledge of the area and people within the places where they live and operate. The information they and seek and obtain is readily available as open source and unclassified information.

d. Criminals. The criminal threat is not as readily apparent to identify. They will collect open source and unclassified information that is publicly available, as well as information they can obtain through various means such as coercion and information they can obtain from insiders of the organization they target. The supporting Criminal Investigative Division (CID) unit may be able to assist both in identifying crime conducive conditions that increase the risk of critical information compromise and in mitigating or eliminating the criminal threat.

e. Hackers. A hacker is a highly skilled computer programmer who specializes in computer and network systems security. Some hackers apply their skills for legitimate uses; however, there are hackers with malicious intent, referred to as crackers, who are motivated by ideology, criminal intent, revenge, thrill-seeking, and/or bragging rights. Malicious crackers can easily obtain information on computer systems and networks and have the skills to penetrate through sophisticated defenses. Hackers are extremely difficult to identify, since they are able to remain hidden and anonymous through the vast expanse of the internet. For these reasons, critical and sensitive information on publicly accessible websites are easy targets for hackers and must not be posted on unclassified computers and networks.

f. Insiders. The insider threat consists of personnel who work inside the organization. They are the most dangerous threat because of their access to information for which they are cleared and the actions they can perform within the organization. They are also very difficult to identify when they can keep their collection activities unnoticed. For these reasons, sensitive and critical information should only be shared with personnel who need to know.

E-3. Threat Collection in the Basic Intelligence Disciplines

Intelligence disciplines are categories of intelligence functions. Although (Joint Publication 2-0, Joint Intelligence) defines these disciplines, it also includes Open-Source Intelligence (OSINT) as a separate intelligence discipline. Being OSINT is more appropriately defined as a category of information, used singly or integrated into an all-source analytical approach, it is not defined in Army doctrine as an intelligence discipline. The Army's intelligence functions are:

a. All-Source Intelligence.

(1) All-source intelligence is a separate intelligence discipline that is defined as the intelligence products, organizations, and activities that incorporate all sources of

information and intelligence, including open-source information, in the production of intelligence. Adversaries seek information from all available sources and will consolidate them into all-source intelligence products.

(2) With the change in the global information environment, OSINT has become a significant source from which adversaries collect information for use against the U.S. Vast amounts of information of great interest to foreign intelligence services and other intelligence collectors are readily available.

(a) OSINT involves the collection and analysis of freely available information, such as that presented in the media, available in libraries, or the internet. Open source information includes photographs, newspapers, magazine advertisements, government and trade publications, contract specifications, congressional hearings, computers, and other public media.

(b) In recent years, the internet has become an ever-greater source of open source information for adversaries, websites in particular, especially personal websites of individual Soldiers (to include blogs), are a potentially significant vulnerability. Other sources for open source information include public presentations, news releases from units or installations, organizational newsletters (both for official organizations and unofficial organizations, such as alumni or spouse support groups), and direct observation.

b. HUMINT. The various adversaries will have an inclination to conduct collection through HUMINT over the other technical collection disciplines. While HUMINT collection can take much longer to conduct, it is low-cost and can yield intangible information that cannot be collected by mechanical means.

(1) The multidiscipline approach to intelligence collection includes the use of human sources to gain access to information not accessible to other collection assets. HUMINT employs overt and clandestine operations to achieve worldwide collection objectives.

(2) Overt collection operations gather intelligence information from open sources. Threat HUMINT collectors include official diplomatic and trade representatives, visitors, exchange students, journalists, and military personnel legitimately in the U.S.

(3) Clandestine collection operations encompass those activities conducted in a manner intended to assure operational secrecy while providing plausible denial for the sponsoring government. These operations target human sources for information not available through open sources.

(a) Clandestine operations are usually expensive and time-consuming. They also involve potential embarrassment to the sponsoring government upon discovery; therefore, the value of the desired information must justify the costs and risks involved.

(b) Clandestine collection activities may be pursued under cover of business or other activities. Attempts may be made to buy material through third parties or directly as a commercial transaction.

(c) Greed, financial gain, alcoholism, drug abuse, sexual perversion, marital infidelity, and financial indebtedness are among the human failures exploited by threat HUMINT collectors. Disenchanted idealists are also a fertile source of information. Another recruitment technique involves misrepresentation of status or the "false flag”

approach. A threat agent will attempt to pass himself off as an agent of a U.S. agency or of a friendly government to solicit cooperation.

c. Imagery Intelligence (IMINT). Adversaries can obtain IMINT from land, sea, air, and space platforms when they operate or have access to these IMINT collection platforms.

(1) The most serious threat at the strategic level stems from photoreconnaissance and open skies observation flights. At the tactical level, airborne collection possesses the greatest IMINT threat. The constant improvement of technical equipment and the employment of combinations of sensors enhance the quality and timeliness of the intelligence product for our adversaries.

(2) Adversaries can gain open source IMINT from commercial companies selling products obtained from commercial IMINT collection platforms as well as from commercially available programs on the internet. Some of the readily available commercial IMINT products may not have all the detail necessary for planning an operation but they provide a foundation of information that adversaries can use.

d. Signals Intelligence (SIGINT). SIGINT incorporates the sub-disciplines of Communications Intelligence (COMINT), Electronics Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT).

(1) COMINT has the greatest impact on the day-to-day performance of Army missions. It derives information from the study of intercepted electromagnetic communications. Prime sources of valuable COMINT include clear voice or non-encrypted telephone and radio communications. Adversaries, especially nation states with intelligence services, use various intercept platforms and have a worldwide COMINT capability. Other adversaries without these sophisticated capabilities will use commercially available technology to obtain COMINT that can be effective when properly utilized.

(2) ELINT is technical or intelligence information derived from non-communications electromagnetic radiations, such as that emitted by radar.

(3) FISINT is derived from the intercept and analysis of electronically transmitted data containing measured parameters of performance, either human or mechanical. Examples are transmitted data on an astronaut's biological status or of a ballistic missile performance.

e. Measurement and Signatures Intelligence (MASINT). MASINT is scientific and technical intelligence obtained by quantitative and qualitative analysis of data derived from technical means for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification or measurement. The six sub-disciplines of MASINT are radar, radio frequency, geophysical, nuclear radiation, materials, and electro-optical. MASINT includes all technical intelligence except SIGINT and overhead imagery. MASINT is more likely to be used by adversaries with access to highly technical and sophisticated equipment.

f. Technical Intelligence (TECHINT).

(1) TECHINT is derived from the collection and analysis of threat and foreign military equipment and associated material for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary’s technological advantages.

(2) Adversaries seek TECHINT on U.S. equipment and material in order to learn their vulnerabilities and counter U.S. technological advantages. As an example, adversaries want to know the vulnerabilities of U.S. vehicles and armor protection in order to conduct effective IED attacks against U.S. forces.

g. CI counters or neutralizes the adversary's intelligence collection efforts through collection, counter-intelligence investigations, operations, analysis and production, and functional and technical services. CI includes all actions taken to detect, identify, track, exploit, and neutralize the multidiscipline intelligence activities of friends, competitors, opponents, adversaries, and enemies. CI is the key intelligence community contributor to protect U.S. interests and equities. CI assists in identifying critical information, identifying vulnerabilities to threat collection, and actions taken to counter collection and operations against U.S. forces.

E-4. Technology Transfer

The acquisition of sensitive technology by adversaries has led to the significant enhancement of their military and industrial capabilities at the expense of the U.S. 50 USC App. 2401-2420 (The Export Administration Act (EAA) of 1979), extended by EO 13222 (Continuation of Export Control Regulations) under the International Emergency Economic Powers Act, addresses this threat by emphasizing the control of critical technology. To accomplish this task, DOD has enacted a series of initiatives to protect U.S. critical technologies. These policies are contained in DOD Directive 5000.1, (Defense Acquisition), and DOD Instruction 5000.2 (Operation of the Defense Acquisition System). The DOD Acquisition Systems Program implements measures to identify and protect U.S. critical technologies from inception to termination of use. The following serves to outline the threat that exists in the illegal transfer of U.S. government technology.

a. "The threat" is actually many threats from many external sources: both governmental and commercial (often working together).

b. The highest targeting priority is given to technology (classified or unclassified), which has direct relevance to economic and strategic advantage.

c. What is being threatened and who is engaging in collection efforts are determined by specific technological interests; our information may be "targeted" by any country or international organization. Members of the scientific and technical community, including engineers (both within and outside of government), are increasingly likely to be singled out as espionage targets.

APPENDIX F

Sample OPSEC Measures

The OPSEC measures in this appendix are only examples to stimulate thought. Do not use them as a checklist. This is not a comprehensive list. Possible OPSEC measures are as varied as the specific vulnerabilities they address.

F-1. Operations and Logistics

a. Randomize the performance of functions and operational missions. Avoid repetitive or stereotyped tactics and procedures for executing operations or activities in terms of time, place, event sequencing, formations, and mission command arrangements.

b. Employ force dispositions and mission command arrangements that conceal the location, identity, and command relationships of major units.

c. Conduct support activities in a way that will not reveal intensification of preparations before initiating operations.

d. Transport supplies and personnel to combat units in a way that conceals the location and identity of the combat units.

e. Operate aircraft at varying altitudes and use random flight routes.

f. Operate to minimize reflective surfaces that units and weapon systems present to radar and sonar.

g. Use darkness to mask deployments or force generation.

h. Approach an objective "out of the sun"' to prevent detection.

i. Randomize convoy routes, departure times, speeds, etc.

j. Do not set patterns to patrolling activities (start times, locations, number of personnel in a patrol, etc.)

k. Do not use same Landing Zone (LZ) or pick-up point repetitively.

l. Do not use same approach (aircraft) or route (vehicle) into and out of an area repetitively.

m. Do not establish over watch, sniper, communications, and medical evacuation/ support positions at the same location every time out.

n. Vary small unit patrol formations; do not set patterns.

F-2. Technical

a. Use radio communications emission control, low probability of intercept techniques, traffic flow security, Ultra-High Frequency (UHF) relay via aircraft, burst transmission technologies, secure phones, landline, and couriers. Limit use of High Frequency (HF) radios and directional Super High Frequency (SHF) transponders.

b. Control radar emissions and operate at reduced power.

c. Mask emissions of forces from radar or visual detection by use of terrain (such as hills and mountains).

d. Maintain noise discipline, operate at reduced power, proceed at slow speeds, and turn off selected equipment.

e. Use camouflage, smoke, background noise, added sources of heat or light, paint or weather.

f. Use deceptive radio transmissions.

g. Use decoy radio or emission sites.

F-3. Administrative

a. Avoid bulletin board plan of the day or planning schedule notices that reveal when events will occur.

b. Conceal budgetary transactions, supply requests and actions, and arrangements for services that reveal preparations for activities.

c. Conceal the issuance of orders, the movement of specially qualified personnel to units, and the installation of special capabilities.

d. Control trash dumping or other housekeeping functions to conceal the locations and identities of units.

e. Destroy (burn, shred, etc.) paper to include unclassified information to prevent the inadvertent disposal of classified and sensitive information.

f. Follow normal leave and pass policies to the maximum extent possible before an operation starts in order to preserve an illusion of normalcy.

g. Ensure personnel discreetly prepare for their family's welfare in their absence and their families are sensitized to their potential abrupt departure.

h. Maximize use of security screening of local national hires and minimize their access and observation opportunities.

i. Randomize security in and around installation/camp to prevent setting pattern or observable routine.

j. Conduct random internal (in camp) unannounced identity and security inspections.

F-4. Military Deception

a. MILDEC can directly support OPSEC by distracting foreign intelligence away from, or provide cover for military operations and supporting activities. MILDEC can be planned and executed by and in support of all levels of command to support the prevention of an inadvertent compromise of classified information and S/CI. OPSEC and MILDEC must be synchronized and deconflicted to ensure that MILDEC is effective and believable.

b. OPSEC can also support MILDEC. An OPSEC analysis of a planned activity or operation identifies potential OPSEC vulnerabilities. Those vulnerabilities are useful to MILDEC planners as possible conduits for passing deceptive information to an adversary. Additionally, MILDEC actions often require specific OPSEC protection. An OPSEC analysis of a planned MILDEC is needed to protect against an inadvertent or unintentional outcome. Failure to maintain good OPSEC can lead to identification of the operation as a deception effort and cause the adversary’s intelligence services to refocus their attention on the actual friendly operation.

F-5. Combat Action

During hostilities, use force against the adversary's ability to collect and process information. This can involve interdiction, sabotage, direct action missions, guerrilla operations, or strikes against adversary targets.

APPENDIX G
OPSEC Relationships to Security Programs

G-1. Background
As stated in Chapter 1, OPSEC protects critical information from adversary observation and collection in ways traditional security programs cannot. While security programs focus on protecting classified information, OPSEC focuses on eliminating, reducing, or concealing the unclassified indicators that can compromise classified information, especially critical information. Despite these differences, OPSEC and security programs are related and must be mutually supporting in order to ensure maximum protection of classified information as well as critical information. The following paragraphs address the relationship of OPSEC to other programs.

G-2. Information Security
a. INFOSEC is the system of policies, procedures, and requirements established under the authority of Executive Order 12958 (Classified National Security Information) and Executive Order 13292 (Further Amendment of Executive Order 12958, As Amended Classified National Security Information), to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

b. AR 380-5 provides guidance for classifying material to prescribe the level of protection afforded to it. Protective measures (such as security containers) deny unauthorized personnel access to classified material. The threat of open source exploitation and possible non-compliance with procedures intended to keep classified material from appearing in open sources are OPSEC concerns.

c. Bits of information conveyed in non-secure radio transmissions, non-secure telephone calls, unencrypted e-mail containing sensitive information, public releases, briefings for the public, friendly conversations in public areas, etc., permit adversaries to piece together U.S. intentions and military capabilities. Implementation of OPSEC measures prevents critical information from appearing in open sources.

G-3. Information Assurance
a. IA is the protection of information systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats. See AR 25-1 and AR 25-2 for more information.

b. IA provides the means to ensure the confidentiality, integrity, and availability of information processed by the Army's information-based systems. It provides a measure of confidence that the security features, practices, procedures, and architectures of an information system accurately mediates and enforces the security policy. IA supports OPSEC by ensuring the confidentiality of information when it is transmitted from the sender to the recipient(s). Confidentiality is the assurance that information is not disclosed to unauthorized entities or processes.

c. IA is the security discipline that encompasses Communications Security (COMSEC), Computer Security (COMPUSEC), and emissions security. See AR 380-40 (Safeguarding and Controlling Communication Security Material).

(1) COMSEC consists of measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. COMSEC is of particular interest to OPSEC. The intercept of non-secure communications is a significant source of intelligence information and OPSEC indicators for adversaries. Components of COMSEC are cryptographic and transmission security.

(a) Cryptographic security is the use of encryption systems to transmit information by message or telephone, which is encrypted or sent using an authorized code. OPSEC is concerned with any deviation from established cryptographic practices that would permit any adversary to "read" U.S. message traffic. OPSEC is also concerned with the possible release of specific information about how friendly cryptographic systems are used or any vulnerabilities that may exist.

(b) Transmission security has a major interface between OPSEC and COMSEC. Transmission security is concerned with the conclusions that can be determined from the externals to a communications signal, the intercept of a signal (such as, deviation of location or identity) and the patterns and volumes of communications from and to various locations. All of these may be OPSEC indicators.

(2) COMPUSEC consists of measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer or AIS. COMPUSEC prevents the intentional or accidental penetration of an AIS. It avoids the disclosure, modification, or destruction of AIS and associated data. Examples are "hacker" penetrations and computer "virus attacks."

(3) EMSEC is concerned with identifying and eliminating unintentional radiation that conveys classified information. In emissions security, TEMPEST refers To Investigations and Studies of Compromising Emanations (TEMPEST)

G-4. Electronic Security

ELSEC is concerned with denying adversaries the information derived from interception and study of non-communications electromagnetic emissions. One part of ELSEC similar to transmission security involves controlling the emissions of radars, navigational aids, and weapons emitters to deny intercepts. Reducing the information content of the emitters to make them more difficult to identify and locate is ELSEC and is also an OPSEC measure.

G-5. Emission Control

Encompasses Controlling (EMCON) all radiation that hostile sensors can detect. A key purpose of EMCON is to prevent detection or identification. EMCON thus crosses the boundaries of OPSEC, COMSEC, ELSEC, and Electronic Warfare (EW).

G-6. Military Deception

MILDEC supports military operations through the application of techniques that simultaneously deny certain true information or indicators and convey or display false

information or indicators that will be accepted by adversaries. MILDEC actions mislead adversaries, causing them to derive and accept desired appreciations of U.S. military capabilities, intentions, operations, and other activities.

a. Depending on the objective, MILDEC can be an OPSEC measure, or OPSEC can support MILDEC. When procedural or physical security means are unavailable for controlling OPSEC vulnerabilities, MILDEC can mislead adversaries, thereby minimizing the OPSEC vulnerability.

b. OPSEC supports MILDEC planners by assisting in determining the indicators the adversary should be allowed to see in order to make the deception appear believable, and determining which indicators of a deception must be protected and how to protect them.

G-7. Physical Security

Physical security consists of protective measures to deny unauthorized personnel access to specific areas, facilities, material, or classified information.

a. By denying access, physical security measures can be OPSEC measures. However, physical security measures can become compromised (for example, combat patrolling at predictable intervals, personnel routinely and predictably leaving a facility unattended, easily seen sensors, changing military police patrols at set times, reacting predictably to alarms, and being careless or lazy in implementing physical security measures).

b. OPSEC can support physical security by identifying actions or indicators an adversary could exploit.

G-8. Force Protection

FP consists of actions taken to prevent or mitigate hostile actions against all DoD personnel (Service Members, Civilians, Contractors, and Family Members), resources, facilities, and critical information. OPSEC plays a vital role in the following ways:

a. OPSEC can identify indicators of routine actions observable by a terrorist that represent a vulnerability both in a tactical environment and in garrison.

b. OPSEC can assist in determining measures to negate terrorist collection of information needed for planning.

c. OPSEC can identify indicators or existing vulnerabilities and recommend OPSEC measures to reduce the likelihood of being attacked.

d. OPSEC can assist FP by ensuring protective measures are in the right place at the right time.

e. OPSEC develops critical information that identifies what must not be allowed to appear in the public domain to prevent collection by a terrorist.

G-9. Program Protection Planning

a. DoDI 5200.39 (Critical Program Information (CPI) Protection) specifies the focus of program protection planning, and shall be identified early in the acquisition life cycle, but not later than Milestone B, or when the program enters the acquisition process. Once CPI has been identified, a PPP is required. Waivers or exceptions are not allowed for this requirement. If no CPI is identified, a PPP is not required.

b. The DoDI 5200.39 references DoDM 5200.01v4 (DoD Information Security Program: Controlled Unclassified Information) as procedural manuals for the development and implementation of PPP. The PPP uses traditional security disciplines and OPSEC to achieve protection.

APPENDIX H
Duty Description for OPSEC Officers and Eligibility Requirements

H-1. Overview
This section discusses the three positions in the OPSEC Program.

H-2. General OPSEC Duties
a. Organize and manage the unit, activity, installation, or organization's OPSEC program to include subordinate OPSEC programs.

b. Identify the organizations critical information, recommend the CIL to the Commander for approval, and publish the CIL.

c. Publish an OPSEC SOP/Plan and ensure OPSEC measures conform to guidance from higher authorities.

d. Maintain awareness of all unit activities, advise appropriate personnel about the organization's OPSEC posture, and offer recommendations to eliminate or reduce vulnerabilities.

e. Conduct OPSEC reviews IAW guidance in this regulation.

H-3. OPSEC Program Manager Duties.
The organization's OPSEC Program Manager administers the Commander's OPSEC Program. An OPSEC Program Manager is responsible for the development, organization, and administration of an OPSEC program at Corps and Installation level and higher. The OPSEC Program Manager provides guidance and oversight to multiple subordinate OPSEC programs of various units, activities, and organizations, and coordinates their actions under the Command's OPSEC Program. OPSEC Program Managers are also OPSEC Officers, but because of the extent and complexity of the OPSEC program they oversee, they are primarily referred to as OPSEC Program Managers.

In addition to H-2:

a. Integrate, coordinate, and synchronize subordinate OPSEC programs.

b. Coordinate with the Army OSE prior to conducting OPSEC Level II Training.

c. Serve as the OPSEC Level III Instructor.

d. Oversee all OPSEC training requirements.

e. Establish OPSEC as an element of the CIP.

f. Conduct OPSEC assessments of own organization and subordinate elements.

g. Interface with all subordinate OPSEC Officers and Coordinators on issues that affect the command.

h. Coordinate with all HHQs.

i. Submit the Annual OPSEC Report to the HHQs OPSEC PM.

j. Maintain contact with Army protection personnel (Continuity of Operations Plan (COOP), AT, HRP, Force Health Protection (FHP), IA, Computer Network Defense (CND), Law Enforcement (LE), Critical Infrastructure Risk Management (CIRM), Emergency Management (EM), Fire & Emergency Services (F&ES), and G-2), and security agencies to obtain information that supports the OPSEC planning process.

k. Coordinate OPSEC planning for FUOPs, exercises, tests, and activities. As required, write OPSEC documents, annexes, and appendices to OPLANs and OPORDs. Write OPSEC documents as required for activities not covered by OPLANs and OPORDs.

l. Organize and provide oversight to an OPSEC OWG. An OWG brings together OPSEC Officers and other security-related positions to ensure the OPSEC program is consistent across the organization and is integrated at the work level. The OWG will assist the OPSEC Officer in developing OPSEC measures and solutions to implementation problems. The working group will provide coordination of all recommendations being forwarded to senior leadership and will assist with development of briefings and reports. The OPSEC Program Manager co-chairs the monthly PWG that has combined all the elements of protection into one working group. The PWG meets 0900-1000 on the second Thursday of each month.

H-4. OPSEC Officer Duties

OPSEC Officers are responsible for the development, organization, and administration of an OPSEC program at Division level and below.

In addition to H-2:

a. Conduct the command's OPSEC Level I Training.

b. Maintain contact and coordination with the next higher echelon OPSEC Officer or OPSEC PM.

c. Where appropriate and as required, conduct OPSEC assessments of subordinate units.

d. Write OPSEC documents, annexes, and appendices to OPLANS and OPORDS. Write OPSEC SOPs/Plans as required for activities not covered by OPLANS and OPORDS.

e. For OPSEC Officers in RDT&E activities, provide specific and tailored OPSEC guidance to activities that are involved in developing system requirements and to associated system development, tests, and evaluations.

H-5. OPSEC Coordinator Duties.

The OPSEC Coordinator has a significant role in the OPSEC program. The OPSEC Coordinator assists the OPSEC PM or OPSEC Officer in the development, organization, and administration of the OPSEC program. Since contractors do not have authority over U.S. military and government personnel and cannot represent the position of the U.S. Government, contract employees will not be assigned as the command's OPSEC Officer. However, they may perform OPSEC duties in a supporting capacity as the OPSEC Coordinator.

H-6. Qualifications for OPSEC PM/Officer/Coordinator

a. Experience and Knowledge.

(1) Operations experience is essential for the positions of OPSEC PM, Officer, and Coordinator.

(2) The OPSEC PM, Officer, or Coordinator should have experience in planning and conducting information gathering, processing, and extracting data from materials, understand the concept of indicators and warnings, and have problem-solving techniques.

(3) The OPSEC PM, Officer, or Coordinator must have thorough comprehension of the functional relationships and procedural processes of the unit or organization.

(4) The OPSEC PM, Officer, or Coordinator must possess working knowledge of the Army and command planning systems, directives, and the organization's plans and procedures.

(5) The OPSEC PM, Officer, or Coordinator must be knowledgeable of traditional security programs and their distinct relationship to OPSEC.

b. Training and Education.

(1) PM are required to attain OPSEC Level II certification and are strongly recommended to attain Level III certification.

(2) OPSEC Officers are required to attain Level II certification and may attain Level III certification based on the recommendation from their chain of command and the OPSEC PM.

(3) OPSEC Coordinators are required at a minimum to complete OPSE 1301 or the equivalent. If executing duties as described in paragraphs H-3 or H-4, the individuals would be performing the duties of an OPSEC Officer and must attend OPSEC Level II certification.

(4) Level II certification must be attained within 90 days of appointment.

c. OPSEC Skills

(1) The OPSEC PM, Officer, or Coordinator must be able to provide advice about policies, doctrine, and guidance and apply effective OPSEC measures.

(2) The OPSEC Program Manager, Officer, or Coordinator must have the ability to integrate and coordinate OPSEC planning with the other capabilities of IO.

d. Communicative Skills.

(1) Ability to independently develop and present clear, concise briefings with sound conclusions and recommendations.

(2) Ability to develop OPSEC awareness training programs and present them to all personnel.

(3) Ability to write and organize concise plans, directives, and training materials.

e. Security Clearance. All OPSEC PMs, Officers, and Coordinators must be eligible to be cleared to the highest level of classified information and accesses required for them to provide OPSEC support to their command or organization. At a minimum, all personnel serving in an OPSEC duty position will have a SECRET clearance.

H-7. OPSEC Officer Eligibility Requirements

a. All Fort Hood organizations that are battalion-sized or higher (commander or director is a O-5 or Civilian equivalent) must have an OPSEC program that is managed by a primary and alternate OPSEC Officer. This requirement applies to tenant units and standalone facilities as well. In order to meet the eligibility requirements, the primary and alternate OPSEC Officers must meet the following:

(1) Must have a secret or higher clearance;

(2) Be designated on appointment orders as the Organization's OPSEC Officer primary or alternate. Appointment orders must be on file with the United States Army Garrison (USAG) OPSEC PM;

(3) Have one-year retainability within the organization (not due to have a Permanent Change of Station (PCS), Estimated Termination of Service (ETS), or retire);

(4) Must have OPSEC Level II training. The training certificate must be on file with the USAG OPSEC PM;

(5) Must have operations experience. OPSEC is an operations function. Personnel in the 35 Series Military Occupational Specialty (MOS) or the S2 section may not be the OPSEC Officer. Since the Antiterrorism Officer (ATO) and OPSEC Officer duties are similar, both duties may be coordinated by the same individual; and

(6) Meet the appropriate rank / grade required for OPSEC Officers:

- Division: Captain (CPT) or above, Chief Warrant Officer (CW)2 or above, Master Sergeant (MSG) or above or General Schedule (GS)-09.
- Brigade: CPT or above, WO1 or above, Sergeant First Class (SFC) or above or GS-09.
- Battalion: 1 Lieutenant (LT) or above, WO1 or above, Staff Sergeant (SSG) or above or GS-07.

b. The positions of OPSEC PM, Officer, or Coordinator are defined:

(1) OPSEC PM. The OPSEC PM is responsible for the development, organization, and administration of an OPSEC program at Corps and/or Installation/ Garrison and higher. The PM provides guidance and oversight to multiple subordinate OPSEC programs of various units, activities, and organizations, and coordinates their actions under the Command's OPSEC Program. PMs are OPSEC Officers, but because of the complexity of the OPSEC program they oversee, they are primarily referred to as OPSEC PMs.

(2) OPSEC Officer. The OPSEC Officer is responsible for the development, organization, and administration of an OPSEC program at Division level and below.

(3) OPSEC Coordinator. The OPSEC Coordinator assists the OPSEC PM or OPSEC Officer in the development, organization, and administration of the OPSEC program. Because contractors do not have the authority over U.S. military, government personnel and cannot represent the position of the U.S. government, contract employees will not be assigned as the Command's OPSEC PM or OPSEC Officer. However, they may perform OPSEC duties in a supporting capacity as the OPSEC Coordinator.

c. The OPSEC PM, Officers, or Coordinators must:

(1) Coordinate with the installation OPSEC PM to attend OPSEC Level II training or if have previously taken, submit training certificate to the installation PM for record.

(2) Attend monthly PWG. The working group is typically held 0900 every second Thursday of each month except when that day falls on a holiday. The location is the W217 conference room in the III Corps HQ building.

(3) Complete and submit quarterly updates to the installation OPSEC PM. These updates include the OPSEC Officer Roster and the OPSEC Training Statistics. The updates are due no later than the last working day of each quarter.
The statistics are reported to the Senior Commander during the Protection Executive Board (PEB) semiannually.

d. Review and sign PWS for new contracts within their organization.

e. Provide OPSEC Level I training annually to unit or track the completion of the online training. The online training can be found at http://cdsetrain.dtic.mil/opsec/index.htm. A certificate is provided at the end of the training.

Appendix I: Program Assessments

The OPSEC Assessment is an analysis of an operation, exercise, test, or activity to determine the overall OPSEC posture. The assessment also evaluates the degree of compliance with the published Fort Hood OPSEC Program and the requirements listed in AR 530-1. The OPSEC Officer conducting the assessment must submit written assessment results and recommendations to the assessed unit commander or director and the OPSEC Officer/Program being assessed. The OPSEC Checklist below was developed to meet the needs of the installation.

Table I-1: OPSEC ASSESSMENT CHECKLIST

OPSEC Assessment Checklist				
Organization:			**Date:**	
Inspector: Carla Stamper			**Phone: 285-5935**	
Code	**Question**	**References**	**Inspector's Comments**	**Corrective Actions**
G3-OPC-OPC-001	Is OPSEC an Operations function?	(AR 530-1, para 1-8a)		
G3-OPC-OPC-002	Does the organization have a OPSEC Plan / SOP?	(AR 530-1, 2-3a (3))		
G3-OPC-OPC-003	Does the organization have a critical information list?	(AR 530-1, 2-2a (1))		
G3-OPC-OPC-004	Has the organization designated an OPSEC officer on appointment orders?	(AR 530-1, 2-3a (1))		
G3-OPC-OPC-005	Is the OPSEC officer knowledgeable of his / her duties?	(AR 530-1, app H-6b)		
G3-OPC-OPC-006	Has the OPSEC officer and other staff personnel been trained per DA Guidance?	(AR 530-1, 4-2b (1))		
G3-OPC-OPC-007	Has the director established OPSEC as a command emphasis item in that it is included in all activities?	(AR 530-1, 2-2a/2-3a (12))		
G3-OPC-OPC-008	Has the director approved the organization's CIL and circulated the list to all subordinates as widely as security classification permits?	(AR 530-1, 2-3a (5))		
G3-OPC-OPC-009	Does the OPSEC program identify specific requirements to plan for and implement OPSEC before, during and after operations and other activities to include RDT&E that affect the combat capability of the U.S. Army?	(AR 530-1, app D-11)		
G3-OPC-OPC-010	Does the OPSEC training program accomplish the following three categories of training? a. Orientation Training b. Awareness Training c. OPSEC Officer Training	(AR 530-1, 4-2a (1,2)/4-2b)		
G3-OPC-OPC-011	Is there an annual review of OPSEC procedures to improve OPSEC programs, include results in annual OPSEC reports up the chain of command?	(AR 530-1, 2-4d)		
G3-OPC-OPC-012	Is a summary of the overall condition of the OPSEC program provided to USAG by 1 Dec of each year?	(AR 530-1, Appendix I)		
G3-OPC-OPC-013	Has the OPSEC Officer developed an OPSEC Working Group? Do they attend the installation OWG?	(AR 530-1, 2-4f)		
G3-OPC-OPC-014	Does each person know the answers to the following questions? a. What is my unit's critical information? b. What critical information am I responsible for? c. How is the threat trying to obtain my critical information? d. What steps am I taking to protect my critical information? e. Who is my OPSEC Officer?	(AR 530-1, 4-2a (1))		
G3-OPC-OPC-015	Are CDR's ensuring annual OPSEC reviews of all organizational websites are conducted and including these results in their annual OPSEC reports?	(AR 530-1, 2-3a (15) (a)/5-2d (1)/AR 25-1)		
G3-OPC-OPC-016	Do contracts receive an OPSEC review of the Statement of Work prior to public release?	(AR 530-1, 6-2b)		
G3-OPC-OPC-017	Is OPSEC incorporated into all classified and unclassified contracts that involve sensitive information?	(AR 530-1, 2-3a)		
G3-OPC-OPC-018	Are FOIA and Privacy Act requests receiving OPSEC reviews?	(AR 530-1, 5-1)		
G3-OPC-OPC-019	Is OPSEC considered in all public affairs operations?	(AR 525-13, app C-4d (4))		
G3-OPC-OPC-020	Does the Web Master coordinate directly with the Command OPSEC Manager for additional guidance as needed on any questionable web site posting?	(AR 25-1, 5-10/AR 530-1, 5-2d)		

Appendix J:
Table J-1: Website Review Checklist

USAG OPSEC Website (WS) Review (IAW AR 25-1 & AR 530-1 OPSEC Reviews will be completed on a quarterly and as requested basis.)			
Reviewer's Name		Date of Review	
Organization Reviewed		Reviewed URL	
WS Overall Score			

Management Controls		
Question	Yes / No	Comment / Corrective Actions
1. Does the WS contain a clearly defined purpose statement that supports the mission of the DoD Component?		
2. Are users of this WS provided with a privacy and security notice prominently displayed or announced on at least the first page of all major sections of each web information service?		
3. If applicable does this WS contain a Disclaimer for External Links notice, when a user request any site outside of the official DoD web information service (usually the .mil domain)?		
4. Is this WS free of commercial sponsorship and advertising?		
5. Is there a link to a page entitled "Contact Us" from the homepage and every major point of entry. Contact information should be generic and include the organization's street address, phone number(s), and email address.		
6. Has the WS administrator completed External Official Presence (EOP) training?		
7. Has the WS administrator attended OPSEC Level II training?		
8. If the WS administrator has attended OPSEC Level II training, is he or she conducting reviews of the WS on a quarterly basis to ensure that each website is in compliance with the policies of AR 25-1 and AR 530-1?		
Operational Information		
9. Does the WS contain any information indicating plans or lessons learned which would reveal military operations, exercises or vulnerabilities?		
10. Does the WS reference any information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program?		
11. Does the WS contain personal information in the following categories about U.S. citizens, DoD employees and military personnel:		
a. Social Security Numbers		
b. Dates of Birth		
c. Home Addresses		
d. Home Telephone Numbers		
e. Names, locations, or any other identifying information about Family Members of DA Civilians or military personnel		
Technological Data		
12. Does the WS contain any technical data such as:		
a. Weapons schematics		
b. Weapon Systems Vulnerabilities		
c. Electronic Wire Diagrams		
d. Frequency Spectrum Data		

Table J-1: Website Review Checklist(continued)

OPSEC Considerations		
13. Does the WS contain relevant information in the following categories that might reveal an organizations plans and intentions?		
a. Administrative		
- Personnel Travel (personal and official business)		
- Attendance at planning conferences		
- Commercial support contracts		
b. Operations, Plans, and Training		
- Operational orders and plans		
- Mission specific training		
- Exercise and simulations activity		
- Exercise, deployment or training schedules		
- Unit relocation/deployment		
- Inspection results, findings, deficiencies		
- Unit vulnerabilities or weaknesses		
c. Communications		
- RF emissions and associated documentation		
- Changes in activity or communications patterns		
- Availability of secure communications		
- Hyperlinks with other agencies or units		
- Family support plans		
- Bulletin board/messages between Soldiers and Family Members		
d. Logistics/Maintenance		
- Supply and equipment orders/deliveries		
- Transportation plans		
- Mapping and imagery		
- Maintenance and logistics requirements		
- Receipt or installation of special equipment		
Key Word Search		
14. Using the following "key words" conduct a search using the search tool. As a result of this search conduct a random screen of any documents found:		
- Deployment Schedules		
- Exercise Plans		
- Contingency Plans		
- Training Schedules		
- Inspection results, findings, deficiencies		
- Biographies		
- Family Support Activities		
- Phone Directories or Duty Rosters		
Other Notes		

Appendix K: Quarterly Reporting

The quarterly updates are due to the OPSEC PM no later than the last working day of each quarter. The spreadsheets identify shortfalls and non-compliancy for Fort Hood units and is provided to the Senior Commander during the semiannual PEB. The PM sends out a reminder and a copy of each spreadsheet at least two weeks in advance for updating. The OPSEC officer will update the spreadsheets and return to the PM. When the OPSEC Officer is on orders to vacate the position (ETS, PCS, retire), he or she will update the PM. The two documents that require updating are:

a. The Fort Hood OPSEC Officer Roster contains every organization on Fort Hood down to the battalion level. Every battalion will have at least one primary and one alternate OPSEC Officer on appointment orders and Level II trained.

(1) The roster update will consist of a strikethrough for any outdated information and an insertion of new data using a different color font.

(2) Information contained on the roster includes (in order as shown below): unit, section, primary /alternate rank, last name, first name, email address, phone number, when the OPSEC Officer received Level II training, if the appointment orders have been received by the PM, total number required, total assigned, total trained and on orders, total on orders only, the percentage of required who have completed requirements (divide on orders and trained by total required), number of coordinators assigned (if any), number of students enrolled in the upcoming course, and any comments

Unit	Section	P/A	Rank	Last	First	Email Address	Phone	Level II Trained	Received Orders	Required	Required Assigned	On Orders & Trained	On Orders Only	Percentage Complete	Coordinators Assigned	Enrolled	Comments
Bde X	Bn 1	P	MAJ	XXX	XXX	XXX	555-0000	6-Aug-14	Yes	4	4	4	0	100%	0	0	
		A	CPT	XXXX	XXXX	XXXX	555-0000	24-Apr-14	Yes								
	Bn 2	P	MAJ	XXXX	XXXX	XXXX	555-0000	27-Feb-14	Yes								
		A	LTC	XXXX	XXXX	XXXX	555-0000	6-Aug-14	Yes								

Figure K-1 Officer Roster

b. The OPSEC Level I Training Statistics tracks the annual OPSEC Level I training statistics for Fort Hood personnel. All Soldiers, Civilians, and Contractors are required to take this training. The update will consist of filling in the required data shown below from: organization, military personnel assigned, Civilian personnel assigned, total personnel assigned, military personnel trained, Civilian personnel trained, total personnel trained, the total percentage trained (divide total trained by the total assigned), and the date of status update. The next section is for Contractors only. If the unit does not have Contractors, this section can be skipped. Fill out the organization, how many Contractors are assigned, how many require the training in accordance with their contracts, how many of the required have been trained, the total percentage (divide total trained by the total required), and
the date of status update.

Soldiers & Civilians								
Organization	Personnel Assigned		Total Assigned	OPSEC Level I		Total Trained	Total %	Status Updated
	MIL	CIV		MIL	CIV			
Unit X	33	129	162	33	129	162	100%	01-Jan-15

Contractors					
Organization	Assigned	Required	Trained	Total %	Status Updated
Unit X	134	134	132	98%	01-Jan-15

Figure K-2 Level I Training Statistics

Appendix L: Compromise Reporting Procedures

1. CUI includes PII, for Official Use Only (FOUO), and Law Enforcement Sensitive (LES) and requires protective measures and controls over access and distribution IAW DoDM 5200.01, Information Security Program, Vol. 4. All users of DoD information systems will protect CUI and prevent unauthorized disclosures. Data spillages will be aggressively monitored, and commanders and supervisors at all levels shall investigate, and when deemed appropriate, discipline those found to have caused or contributed to such incidents. A spillage occurs whenever CUI is transferred onto an information system not authorized for the appropriate security level or not having the required CUI protection or access controls. A spillage creates the potential for further widespread unauthorized disclosure of that information, including to the Internet.
2. In order to prevent unauthorized disclosure of sensitive and/or critical information IAW AR 530-1: (1) do not publicly disseminate or publish photographs displaying sensitive and/or critical information (2) do not publicly reference, disseminate, confirm, publish, or further propagate sensitive and/or critical information that has already been compromised, as this provides further unnecessary exposure of the compromised information and may serve to validate it. Information contained on the III Corps and Fort Hood CIL (see attached CIL) should also be protected at all times. A failure to comply with these directives may be punished as violations of a lawful punitive order under Article 92 of the UCMJ or under other disciplinary, administrative, or other actions as applicable. Personnel not subject to the UCMJ who knowingly, willfully, or negligently fail to protect sensitive

and/or critical information from unauthorized disclosure may be subject to administrative, disciplinary, contractual, or criminal action.

a. Report all OPSEC compromises through the Installation Operations Center (IOC) IAW the Commander's Critical Information Requirements (CCIR). The Fort Hood OPSEC Manager should be included on these emails and a Serious Incident Report (SIR) should be completed and sent to the IOC.

b. The type of incident and the severity will determine the follow on action that should be taken.

3. PII is information that can be used to trace an individual's identity and must be kept private to safeguard that individual's identity, for example, a person's name, social security number, birthday, mother's maiden name, biometric records, home phone number, other demographic, personnel, medical, and financial information. This information should only be made available to people with an official need to know. When there is a PII incident, or, when this information is given to people without an official need to know, an individual's identity is at risk of being stolen. PII can be compromised many ways to include but not limited to stolen or lost computers, hard drives, or thumb drives, through email, or hard copies sent to unauthorized recipients, information posted to public websites, or thrown into the trash. If PII is found through any of the various ways, the following must occur.

a. Report all incidents within one hour of discovery to http://www.us-cert.gov. If computer access is not available, PII incidents can be reported to a 24/7 toll free number at 1-866-606-9580 from the Office of the Administrative Assistant (OAA) to the Secretary of the Army or US Computer Emergency Response Team (US-CERT) at (703) 235-5110 which is also monitored 24/7. On most instances, the individual discovering the incident should report directly to the US-CERT in order to meet the one-hour timeline.

b. The Army has developed a new breach-reporting tool: the Privacy Act Tracking System (PATS). This web-based tool allows organizations to enter and track breaches online. PATS simplifies and improves data collection Army-wide when reporting breaches of PII. Effective 1 October 2015, all Army breach reporting will be required to be conducted through PATS, the Records Management and Declassification Agency website for Army-wide use. Should you have any questions or comments concerning PATs, please send them to usarmy.belvoir.hqda-oaa-aha.mbx.rmda-foia-privacy-alert@mail.mil. Using Common Access Card (CAC) login credentials, report all incidents involving actual or suspected breaches / compromises of PII to the HQ Army privacy Office within 24 hours of discovery at https://www.privacy.army.mil/PATS/. This email should include the US-CERT reporting number, provide a brief synopsis, and contact information for the incident.

c. Continue to follow existing internal command procedures to notify local command officials. This includes but is not limited to SIRs, contacting the Regional Computer Emergency Response Team (RCERT) and Army Computer Emergency Response Team (ACERT) for network intrusion incidents, and notification of Credit Card Company, local law enforcement, FOIA/Privacy Act

officials, and the Public Affairs Office. Internal command notification may not delay the one-hour US-CERT or 24-hour Army FOIA/Privacy Act office reporting requirements.

d. The organization responsible for safeguarding the PII at the time of the incident must notify the affected individuals. IAW Department of Defense Memorandum, Safeguarding Against and Responding to the Breach of PII, 21 Sep 07, low/moderate/ high risk or harm determinations and the decision whether notification of individuals is made, rests with the head of the Army command/agency where the breach occurred; however, all determinations of high risk/harm require notification. When the actual Army activity where the incident occurred is unknown, by default the responsibility for reporting the incident and notification of affected individuals lies with the originator of the document or information. Notification should be made by an individual at a senior level (i.e., commander, director) to reinforce to impacted individuals the seriousness of the incident. More information to include a sample notification letter is available at https://www.rmda.army.mil/privacy/RMDA-PO-Infractions.html

e. Commanders and supervisors will ensure the appropriate remedial action(s) are taken when PII is lost or compromised. At a minimum, if PII is lost because of negligence or failure to follow established procedures, the individual(s) responsible will receive counseling and additional training reminding them of the importance of safeguarding PII. Additional remedial actions may include prompt removal of authority to access information or systems from individuals who demonstrate a pattern of error in safeguarding PII as well as other administrative or disciplinary actions as determined appropriate by the commander or supervisor.

Glossary
Section I
Abbreviations

ACERT
Army Computer Emergency Response Teams

AIS
Automated Information System(s)

AR
Army Regulation

AT
Antiterrorism

ATO
Antiterrorism Officer

CAC
Common Access Card

CALI
Capabilities, Activities, Limitations, and Intentions

CCIR
Commander's Critical Information Requirements

CI
Counter Intelligence

CID
Criminal Investigation Division

CIL
Critical Information List

CIP
Command Inspection Program

CIRM
Critical Infrastructure Risk Management

CND
Computer Network Defense

CNO
Computer Network Operations

COA
Course of Action

COMINT
Communications Intelligence

COMSEC
Communications Security

COMPUSEC
Computer Security

COOP
Continuity of Operations Plan

CPI
Critical Program Information

CPT
Captain

CUI
Controlled Unclassified Information

CW
Chief Warrant Officer

DA
Department of The Army

DCS
Deputy Chief of Staff

DEFCON
Defense Readiness Condition

DoD
Department of Defense

DoDD
Department of Defense Directive

DPTMS
Directorate of Plans, Training, Mobilization, and Security

DTG
Date Time Group

EAA
Export Administration Act

EAR
Export Administration Regulations

ELINT
Electronics Intelligence

ELSEC
Electronic Security

EM
Emergency Management

EMCON
Emission Control

EMSEC
Emission Security

EO
Executive Order

EOD
Explosive Ordnance Disposal

EOP
External Official Presence

ETS
Estimated Termination of Service

EW
Electronic Warfare

FDO
Foreign Disclosure Officer

F&ES
Fire and Emergency Services

FHP
Force Health Protection

FIS
Foreign Intelligence Service

FISINT
Foreign Instrumentation Signals Intelligence

FOIA
Freedom of Information Act

FOUO
For Official Use Only

FP
Force Protection

FPCON
Force Protection Condition

FRG
Family Readiness Group(s)

FRSA
Family Readiness Support Assistant

FUOPS
Future Operations Planning

GCA
Government Contracting Activity

GS
General Schedule

HF
High Frequency

HHQ
Higher Headquarters

HQ
Headquarters

HQDA
Headquarters, Department of the Army

HRP
High Risk Personnel

HUMINT
Human Intelligence

IA
Information Assurance

IAW
In Accordance With

IBC
Internet-based Capabilities

IED
Improvised Explosive Device

IEMP
Installation Emergency Management Program

IG
Inspector General

IMCOM
Installation Management Command

IMINT
Imagery Intelligence

INFOCON
Information Condition

INFOSEC
Information Security

IO
Information Operations

IOSS
Interagency OPSEC Support Staff

ISR
Intelligence, Surveillance, and Reconnaissance

IOC
Installation Operations Center

ITAR
International Traffic In Arms Regulations

JOSE
Joint OPSEC Support Element

LE
Law Enforcement

LNO
Liaison Officer

LOC
Lines of Communication

LT
Lieutenant

LZ
Landing Zone

MASINT
Measurement and Signatures Intelligence

MDMP
Military Decision Making Process

MILDEC
Military Deception

MISO
Military Information Support Operations

MOS
Military Occupational Specialty

MSG
Master Sergeant

MTOE
Modified Table of Organization and Equipment

NEC
Network Enterprise Center

NCO
Non-Commissioned Officer

NISPOM
National Industrial Security Program Operating Manual

NSDD
National Security Decision Directive

OAA
Office of the Administrative Assistant

OPLAN
Operation Plan

OPORD
Operations Order

OPSEC
Operations Security

OSE
OPSEC Support Element

OSINT
Open-Source Intelligence

OWG
OPSEC Working Group

PA
Public Affairs

PAIO
Plans, Analysis, and Integration Office

PAO
Public Affairs Officer

PCS
Permanent Change of Station

PEB
Protection Executive Board

PII
Personally Identifiable Information

PERSEC
Personnel Security

PEO
Program Executive Officer

PM
Program Manager

PMO
Provost Marshall Officer

PPP
Program Protection Plans

PATS
Privacy Act Tracking Systems

PWG
Protection Working Group

PWS
Performance Work Statement(s)

R&D
Research and Development

RA
Requiring Activity

RDT&E
Research, Development, Test, and Evaluation

RCERT
Regional Computer Emergency Response Team

ROE
Rules of Engagement

RUF
Rules for the Use of Force

SAP
Special Access Program

SCG
Security Classification Guide

S/CI
Sensitive and/or Critical Information

SCI
Sensitive Compartmented Information

SFC
Sergeant First Class

SIR
Serious Incident Report

SHF
Super High Frequency

SIGINT
Signals Intelligence

SNS
Social Networking Site

SOP
Standard Operating Procedure

SOO
Statement of Objectives

SOW
Statement of Work

SSG
Staff Sergeant

TARP
Threat Awareness Reporting Program

TDA
Table of Distribution and Allowances

TDY
Temporary Duty

TECHINT
Technical Intelligence

TEMPEST
Refers to investigations and studies of compromising emanations, in emissions security

TTP
Tactics, Techniques, and Procedures

UCMJ
Uniform Code of Military Justice

UHF
Ultra-High Frequency

U.S.
United States

USAG
United States Army Garrison

US-CERT
US Computer Emergency Response Team

VIP
Very Important Person

WMD
Weapons of Mass Destruction

WS
Websites

Section II
Terms

Adversary
Individuals, organizations, or countries that must be denied critical information in order to preserve mission integrity and maintain friendly mission effectiveness and the element of surprise.

Classified military information
Information originated by or for the DOD or its agencies or under their jurisdiction or control that requires protection in the interest of national security. It is designated TOP SECRET, SECRET, or CONFIDENTIAL as described in EO 13526(Classified National Security) or subsequent order. Classified military information may be in oral, visual, documentary, or materiel form.

Collection Threat
Collection of information on U.S. Army activities may be conducted by adversaries using various intelligence collection methods. These pieces of information provide an accurate portrayal of the commands overall intentions and / or operations.

Communications Security (COMSEC)
Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. The loss of U.S. COMSEC information and materials can seriously damage the national interest.

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

Controlled Unclassified Information (CUI)
Unclassified information to which access or distribution limitations have been applied according to national laws, policies, and regulations of the United States Government (U.S. Government). It includes U.S. information that is determined to be exempt from public disclosure according to (DoDD 5230.25), DoDD 5400.7, AR 25-55, AR 340-21, AR 530-1, and so on, or that is subject to export controls according to the ITAR or the Export Administration Regulations (EAR).

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

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

Critical Information
Critical information is defined as information important to the successful achievement of U.S. objectives and missions, or which may be of use to an adversary of the U.S. critical information consists of specific facts about friendly capabilities, activities, limitations (includes vulnerabilities), and intentions needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishment. Critical information is information that is vital to a mission that if an adversary obtains it, correctly analyzes it, and acts upon it will prevent or seriously degrade mission success. Critical information can be classified information or unclassified information. Critical information can also be an action that provides an indicator of value to an adversary and places a friendly activity or operation at risk.

Critical Information List (CIL)
The CIL is a consolidated list of a unit or organization's critical information. The CIL will be classified if any one of the items of critical information is classified.

Critical Program Information (CPI)
Elements or components of an Research, Development, and Acquisitions program that, if compromised, could cause significant degradation in mission effectiveness; shorten

the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. See DODI 5200.39 for more information.

Defense Critical Infrastructure
The composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide.

Defense Critical Infrastructure Program
A DoD risk management program that seeks to ensure the availability of Defense Critical Infrastructure.

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

Essential Secrecy
The condition achieved from the denial of critical information to adversaries. Adversaries in possession of critical information can hinder or prevent friendly mission accomplishment. Thus, essential secrecy is a necessary prerequisite for effective operations.

For Official Use Only (FOUO)
A designation that is applied to unclassified information that may be exempt from mandatory release to the public under the FOIA.

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

Freedom of Information Act (FOIA)
Allows people to gain access to non-classified information from government agencies.

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

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

Human Intelligence Threat (HUMINT)
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.

Imagery Intelligence Threat (IMINT)
Collection of information by photographic, infrared, or radar imagery. Images can be gathered either 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. The IMINT includes unauthorized duplication of documents.

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

Information Assurance (IA)
The protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats. IA encompasses COMSEC, COMPUSEC, and control of compromising emanations.

Information Operations (IO)
Information operations is the employment of the core capabilities of EW, Computer Netwrok Operations (CNO), MISO, MILDEC, and OPSEC, in concert with specified and related capabilities, to affect or defend information and information systems, and to influence decision-making.

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

Information system (IS)
Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and that includes computer software, firmware, and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems and associated equipment.

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

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

Intelligence System
Any formal or informal system to manage data gathering, to obtain and process the data, to interpret the data and to provide reasoned judgments to decision makers as a basis for action. The term is not limited to intelligence organizations or services but includes any system, in all its parts, that accomplishes the listed tasks.

Internet
The global collaboration of data networks that are connected to each other, using common protocols to provide instant access to the information from other computers around the world.

Measurement and Signature Intelligence (MASINT)
Scientific and technical intelligence obtained by quantitative and qualitative analysis of data derived from technical sensors to identify any distinctive features associated with the source, emitter, or sender. It is technical in nature.

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

Military Information Support Operations (MISO)
Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of MISO is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

Multidiscipline counterintelligence analysis
The process of determining the presence and nature of the total all-source adversary intelligence threat to a given targeting order to provide a basis for countering or degrading the threat.

Observables
Actions that convey indicators exploitable by adversaries but that must be carried out regardless, to plan, prepare for and execute activities.

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

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

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

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

OPSEC Assessment
OPSEC assessment is the analysis of an operation, activity, exercise, or support function to determine the overall OPSEC posture and degree of compliance with HHQs guidance. Assessments shall be conducted on a non-attribution basis and not used as a punitive tool.

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

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

a. Action control. The objective is to eliminate indicators or the vulnerability of actions to exploitation by adversary intelligence systems. Select what actions to undertake; decide whether to execute actions and determine the "who," "when," "where," and "how" for actions necessary to accomplish tasks.

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

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

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

OPSEC Survey
Conducted on at least annually basis, this is part of an overall IO vulnerability assessment, consisting of an intensive application of the OPSEC process to an existing operation or activity by the OPSEC program manager with the support of a multi-disciplined team of experts, thereby identifying requirements for additional measures and for making necessary changes in existing measures.

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

Protection Working Group (PWG)
A cross-functional standing organization, that convenes at least monthly to conduct Antiterrorism, Protection and OPSEC planning and to assess the Protection Program.

Publicly Accessible Website
An Army website with access unrestricted by password or Public Key Infrastructure user authorization. "Public" refers to the at-large audience on the Internet - anyone who can access a website through a browser.

Red Team
An independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities in order to improve the security posture of a unit or organization to include its personnel, equipment, and information systems. Red team methods, also known as red teaming, can reveal the limitations and vulnerabilities of an OPSEC program. Red teaming operates from an adversary's perspective accompanied by innovative and unconventional thinking and can be effective in revealing limitations and weaknesses that are not obvious or apparent to a unit or organization. Red Teams are certified by the National Security Agency

Requiring Activity (RA)
An organization that has a requirement for goods and / or services and requests the initiation of, and provides funding for, an assisted or direct acquisition to fulfill that requirement.

Security Manager
A properly cleared individual having professional security credentials to serve as the manager for an activity. See AR 380-5 for basic responsibilities. Also, refer to AR 380-381(C) for security managers of special access programs.

Sensitive Activities
Sensitive activities are special access or code word programs, critical research and development efforts, operational or intelligence activities, cover, special plans, special

activities, sensitive support to non-Army agencies and/or activities excluded from normal staff review and oversight.

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

Sensitive Compartmented Information (SCI)
Information or material requiring special controls for restricted handling within compartmented intelligence systems and for which compartmentalization is essential. SCI rules are established by the Director of Central Intelligence and are covered in the Sensitive Compartmented Information (SCI) Administrative Security Manual [DoDM 5105.21v1]

Signals Intelligence (SIGINT)
Collection of information by interception of electronic signals from communications equipment or non-communicative devices that emit an electronic signal, such as a rada beacon. It includes interception of communication and the interception and analysis of communication between pieces of equipment (e.g., LAN).

Sources of Data
Materials, conversations, and actions that provide information and indicators. The sources are as follows:

a. Protected sources. Friendly personnel, documents, material and so forth, possessing classified or sensitive data which are protected by personnel, information, physical, crypto, emission and computer security measures.

b. Open sources. Oral, documentary, pictorial, and physical materials accessible to the public.

c. Detectable actions. Physical actions or entities and emissions or other phenomena that can be observed, imaged or detected by human senses or by active and passive sensors.

Sensitive Information
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 which 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 (Computer Security Act of 1987 [Public Law 100-235])

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

Threat
Capability of a potential adversary to limit or negate mission accomplishment or to neutralize or reduce the effectiveness of a current or projected organization or material item. Two types of threat information are required:

a. Intelligence collection threat (efforts by adversary to gain information).

b. Combat capability threat (adversary forces' weapons systems that the U.S. Army will face on the battlefield).

Vulnerabilities
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; adversary has capability to collect indicator, and adversary has time to process (report, analyze, take planning action), and the adversary must be able to react.

Vulnerability Assessment
Vulnerability assessments identify and analyze OPSEC weaknesses, systematically determining the effectiveness of OPSEC in a particular area of an existing operation, activity, or exercise from the viewpoint of an adversary.