Army Regulation 530–1

Operations and Signal Security

Operations Security (OPSEC)

Distribution Restriction Statement.
This publication contains technical or operational information that is for official Government agencies and their contractors. Requests from outside U.S. Government agencies for release of this publication under the Freedom of Information Act or the Foreign Military Sales Program must be made to HQDA (DAMO-ODL-CBT), 400 ARMY PENTAGON, WASHINGTON, DC 20310–0440.

Destruction Notice.
Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Headquarters
Department of the Army
Washington, DC
27 September 2005

UNCLASSIFIED

SUMMARY of CHANGE

AR 530–1
Operations Security (OPSEC)

This rapid action revision, dated 27 September 2005--

- Emphasizes OPSEC guidelines with which all Army personnel will comply.

- Adds and removes responsibilities (chap 2).

- Adds definition of OPSEC Compromise (glossary).

- Redefines Sensitive Information throughout the publication.

- Updates addresses and office symbols throughout the publication.

- Corrects typographical errors throughout the publication.

This revision--

- Implements Department of Defense Directive 5205.2, Operations Security Program policy and joint policy and doctrine in CJCS Instruction 3213.01.

- Fully defines OPSEC as an element of Command and Control Warfare (C2W).

- Outlines OPSEC application for on-site inspections under Intermediate-Range Nuclear Forces (INF), Strategic Arms Reduction Treaty (START), and Chemical Weapons Convention (CWC) agreements.

- Requires battalion level and higher echelons to plan and implement OPSEC programs. Defines battalion level as an organization MTOE/TDA, headed by a lieutenant colonel or a civilian in the grade of GS-13 or higher.

- Updates Review, Assessment and Survey Requirements.

- Includes OPSEC procedures for Special Access Programs.

- Includes sample OPSEC measures, model outline for an OPSEC Plan, and a format for an OPSEC annex to OPLANS/OPORDS.

Headquarters
Department of the Army
Washington, DC
27 September 2005

***Army Regulation 530–1**

Effective 7 October 2005

Operations and Signal Security

Operations Security (OPSEC)

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:

Sandra R. Riley

SANDRA R. RILEY
Administrative Assistant to the
Secretary of the Army

History. This is a rapid action revision. The portions affected by this rapid action revision are listed in the summary of change.

Summary. This regulation on operations security fully implements Chairman, Joint Chiefs of Staff Instruction 3213.01, Joint Publication 3–54, and DOD Directive 5205.2. This revision states Army policy on OPSEC program development, revises terminology, provides details on the OPSEC planning process, and outlines the OPSEC review, assessment, and survey.

Applicability. This regulation applies to the Active Army, the Army National Guard, the United States Army Reserve and related activities of those organizations. It applies to contractors who participate in the DOD Industrial Security Program to comply with contractually imposed OPSEC requirements. This regulation applies during mobilization.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, G-3/5/7 is the proponent of this regulation. The Deputy Chief of Staff, G-3/5/7 has the authority to approve exceptions to this regulation that are consistent with controlling law and regulations. The proponent may delegate the approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army management control process. This regulation contains management control provisions in accordance with AR 11–2, but it does not identify key management controls that must be evaluated.

Supplementation. Supplementation of this regulation and establishment of command or local forms are prohibited without prior approval from HQDA (DAMO–ODL–CBT), Washington, DC 20310–0440.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (DAMO–ODL–CBT), Washington, DC 20310–0440.

Distribution. Distribution of this publication is available in electronic media only and is intended for command levels B, C, D, and E for the Active Army, the Army National Guard, and the United States Army Reserve.

Distribution Restriction Statement.
This publication contains technical or operational information that is for official Government agencies and their contractors. Requests from outside U.S. Government agencies for release of this publication under the Freedom of Information Act or the Foreign Military Sales Program must be made to HQDA (DAMO-ODL-CBT), 400 ARMY PENTAGON, WASHINGTON, DC 20310–0440.

Destruction Notice.
Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Contents (Listed by paragraph and page number)

*This publication supersedes AR 530–1, dated 3 March 1995.

Contents—Continued

Contents—Continued

Appendixes

Figure List

Contents—Continued

Glossary

Index

Chapter 1
Introduction

1–1. Purpose

This regulation prescribes policy and procedures for operations security (OPSEC) in the Army.

1–2. References

Required and related publications and prescribed and referenced forms are listed in Appendix A.

1–3. Explanation of abbreviations and terms

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

1–4. Responsibilities

All responsibilities are listed in chapter 2.

1–5. Requirement

a. The national operations security program requires each executive department and agency with a national security mission to have an OPSEC program. Department of Defense (DOD) Directive 5205.2, DOD Operations Security Program, supports the national program and requires each DOD component to have an OPSEC program.

b. Operations security maintains essential secrecy, which is the condition achieved by the denial of critical information to adversaries. Adversaries in possession of critical information can prevent friendly mission accomplishment. (See para 3–4 for discussion of critical information.) Thus, essential secrecy is a necessary prerequisite for effective operations. Essential secrecy depends on the combination of two approaches to protection:

(1) Security programs to deny adversaries classified information.

(2) Operations security to deny adversaries critical information, which is always sensitive and often unclassified.

c. Operations security provides a way to manage risk. It is impossible to protect everything. To attempt complete protection diverts resources from actions needed for mission success.

1–6. Application

Operations security takes a systematic look at an operation from the adversary’s viewpoint. This approach, developed during the war in Vietnam, proved highly successful. It is widely applicable to combat training and other operations.

a. The Army OPSEC program is consistent with joint policy and doctrine in CJCS INST 3213.01 and Joint Pub 3–54. In joint operations, OPSEC is an element of command and control warfare (C2W).

(1) Command and control warfare integrates OPSEC, military deception, psychological operations (PSYOP), electronic warfare, (EW) and physical destruction. This denies information to, influences, degrades or destroys enemy command and control (C2) capabilities. It protects friendly C2 capabilities against such actions.

(2) Operations security denies adversaries information about friendly intentions and capabilities, which they need to make competent decisions. Without prior knowledge of friendly actions, adversary leaders cannot act effectively to prevent friendly mission accomplishment.

b. Operations security contributes directly to the Army’s ability to field forces superior to an adversary in peace, crisis, or war. Without critical information about our forces, adversaries can not design and build systems, devise tactics, train, or otherwise prepare their forces (physically or psychologically) in time to effectively counter the Army’s capabilities or intentions.

c. Combat capability increasingly depends on the information technology revolution. This impacts all aspects of military and science to raise, equip, train, deploy, employ, and sustain forces. Every Army organization produces or has information that ultimately affects the ability of U.S. forces to do a mission. Every organization, therefore, must identify and protect information an adversary could use to defeat U.S. forces, if that adversary possessed it in a timely manner.

d. Research, development, test and evaluation (RDT&E) activities are particularly vulnerable to the loss of sensitive or critical technology. Recent studies revealed that seventy five percent of U.S. acquisition programs had countermeasures initiated against them within three years of the start of full-scale development. Fifty percent of the programs had countermeasures fielded against them within three years of initial operational capability. Acquisition systems protection is necessary to preserve the advantage of technological surprise for U.S. forces. The use of operations security surveys shall be used to monitor information loss during system development, between each milestone, as a minimum.

e. Many businesses that compete in the global economy are seeking certification according to the International Standards Organization’s ISO 9000 Program. This program certifies that a business meets stringent quality standards. Its inspections are very intrusive. It is very difficult for DOD contractors to protect sensitive information in this environment.

f. The U.S. government is a party to various arms control agreements, which allow access by foreign officials to U.S. military installations and supporting contractor facilities.

(1) Intermediate-Range Nuclear Forces (INF), Strategic Arms Reduction Treaty (START), and Chemical Weapons Convention (CWC) agreements have provisions for on-site inspections. Under CWC, challenge inspections may occur at sites and in buildings that have nothing to do with declared chemical weapons activity. (For example, with only 72 hours of advanced notice, Open Skies will allow reconnaissance over flights anytime, anywhere, with no exceptions.)

(2) These agreements, while enhancing U.S. national security, provide adversaries with opportunities to collect sensitive or critical information unrelated to the treaties. Each Army organization or activity must have an OPSEC plan to protect sensitive and critical information, unrelated to legitimate inspection aims. The plan must direct immediate implementation of OPSEC measures for daily vulnerabilities. This may help to avoid targeting of sensitive activities, unrelated to the treaties, for inspection. The plan will also have additional measures that are specific for a particular inspection regime. These additional OPSEC measures must be ready for implementation after notice of an impending inspection.

1–7. Proponent

As part of C2W, OPSEC is an operations function. It is not a security function, although it requires close integration with security programs, which protect classified information. The operations officer is the staff proponent for OPSEC.

a. The operations officer must consider OPSEC in all unit activities to maintain operational effectiveness. Unit actions are a primary source of indicators collected by adversary intelligence Systems. The operations officer controls these actions. He also assigns tasks and allocates resources to implement other OPSEC measures (see para 3–6) to maintain surprise. Since he constantly monitors activities, he can evaluate these measures for their effectiveness and their impact on operational efficiency.

b. In an organization without a specified operations staff, the element with primary responsibility for planning and controlling activities that accomplish the main mission is the proponent for OPSEC.

c. The operations element is the proponent, but the entire staff must integrate OPSEC into planning and execution of the organization's activities. Military operations are complex; so various functional areas provide indicators of future operations. This makes many aspects of unit activities vulnerable to adversary intelligence services. All staff functions must support the process to defeat them.

d. The intelligence staff element provides intelligence threat assessments tailored to the specific operation or activity under consideration. It works with each of the other staff elements to identify OPSEC vulnerabilities and recommend OPSEC measures. It can also provide expertise in various security disciplines for OPSEC assessments and surveys.

Chapter 2
Responsibilities

2–1. All commanders at battalion and higher echelons

a. OPSEC is a command responsibility. Commanders and agency heads will ensure that their organizations plan and implement appropriate OPSEC measures to preserve essential secrecy in every phase of *an* operation, exercise, test, or activity. *Note.* For purposes or this regulation, an organization is at battalion or higher echelon when its head is a lieutenant colonel, a civilian grade GM- 14, or a higher grade. This regulation applies to any unit authorized by either a modified table of organization and equipment (MTOE) or a table of distribution and allowances CTA).

b. Commanders will develop and implement OPSEC programs to meet their specific needs and to support the OPSEC programs of higher echelons. They will—

(1) Ensure their programs include the common features in paragraph 3–2.

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

(3) Approve the organization's essential elements of friendly information (EEFI). Circulate the list to all subordinates as widely as security classification permits.

(4) Weigh the risks to the mission against the costs of protection and decide what OPSEC measures to implement. Publish such measures in all operations plans (OPLANs) and operations orders (OPORDs) or in an OPSEC plan (for non-tactical activities).

2–2. MACOM commanders

a. MACOM commanders will ensure that command OPSEC programs are examined as part of the Organizational Inspection Program (OIP) outlined in AR 1–201.

b. MACOM commanders at echelons corps and below (ECB) with organic intelligence and counter-intelligence (CI) capabilities will provide intelligence and CI support to OPSEC for ECB units.

2–3. Commander, U.S. Army Information Systems Command

The Commander, U.S. Army Information Systems Command (USAISC) will—

a. Ensure the planning and implementation of OPSEC throughout the life cycle management of USAJSC supported systems.

b. Ensure that system proponents provide EEFI for all Systems to be supported by USAISC at the time support is requested.

2–4. Commander, U.S. Army intelligence and Security Command

The Commander, U.S. Army Intelligence and Security Command (INSCOM) will—

a. Provide intelligence and counterintelligence support to OPSEC for echelons above corps (EAC). Intelligence support includes specialized, integrated, multidiscipline threat and vulnerability analysis. The INSCOM elements will provide information updates, but they do not write threat assessments for the supported command or agency. (The supported organization's intelligence staff element normally performs this function.) The extent of OPSEC support to EAC will depend on the HQDA determined sensitivity of the supported activity and the threat posed by foreign collection assets.

b. Assist in OPSEC surveys, at the request of supported commands.

c. Advise and assist supported commands in electronic warfare (EW) matters and provide technical support to manipulative electronic deception (MED) activities that relate to OPSEC.

d. Provide counterintelligence support to OPSEC at EAC and assist at corps and below as resources permit.

e. Coordinate requests from supported commands for security service assistance to avoid duplication of effort.

f. Provide all source threat evaluation of foreign intelligence organizations.

g. Prepare and provide multidiscipline threat data to supplement threat data obtained by supported commands' intelligence staffs according to AR 381–11. (See app E for collection disciplines.)

2–5. Commander, U.S. Army Materiel Command

The Commander, U.S. Army Materiel Command (AMC) will—

a. Ensure that all AMC research, development and acquisition programs support and effectively implement OPSEC principles and procedures.

b. Provide centralized management and coordination of the AMC OPSEC program.

c. In coordination with U.S. Army Training and Doctrine Command (TRADOC) and USAISC, ensure that a consistent and effective level of OPSEC protection is applied to all systems in life cycle testing and development.

d. In coordination with the Chief of Engineers, provide camouflage and deception research and development for fixed installations, range and test facilities under the cognizance of AMC.

e. Incorporate OPSEC into appropriate contractual agreements.

2–6. Commander, U.S. Army Space and Strategic Defense Command

The Commander, U.S. Army Space and Strategic Defense Command (USASSDC) will—

a. Provide assistance to Headquarters, Department of the Army (HQDA), Office of the Deputy Chief of Staff for Operations and Plans (HQDA ODCS, G-3/5/7) in the development of OPSEC training programs and materials for the Department of the Army.

b. Maintain for HQDA a reference repository for OPSEC training materials relating to OPSEC training programs provided by HQDA ODCS, G-3/5/7.

2–7. Commander, U.S. Army Training and Doctrine Command

The Commander, U.S. Army Training and Doctrine Command (TRADOC) will—

a. Designate a TRADOC proponent for OPSEC.

b. Provide OPSEC doctrine and concepts in Army-wide training literature.

c. Ensure that adequate OPSEC instruction is included in all initial entry training programs at Army training centers and Army service schools. Ensure continuous and progressive OPSEC training for Army personnel throughout their careers and for civilian employees during their periods of employment.

d. Integrate OPSEC in appropriate Army Training and Evaluation Programs (ARTEPs), and in related doctrinal and training publications.

e. Assist HQDA and AMC in the integration of deception and counter surveillance measures into OPSEC.

f. Ensure that OPSEC measures are incorporated into Army combat development activities to include concepts for doctrine, organizations and material.

g. Coordinate with AMC and USAISC to ensure that a consistent and effective level of OPSEC protection is applied to all Systems in life cycle development.

2–8. Commanders, Major Test Ranges and Facilities

The Commanders of range and test facilities will—

a. Publish a written range or test facility OPSEC program and make it available to range users.

b. Obtain the EEFI and the OPSEC plan for each program, project, or activity using the range or test facility. Review them to ensure that activities of one user will not compromise OPSEC measures of another user.

c. Coordinate OPSEC measures between all range and test facility users. Assist users to implement OPSEC measures.

2–9. Program Executive Officers (PEOs) and Program Managers/Project Managers/Product Managers (PMs)

a. Program Executive Officers (PEOs) and Program Managers/Project Managers/Product Managers (PMs) will submit program protection plans for review by the Defense Acquisition Board (DAB) or the Army Systems Acquisition Review Council (ASARC) at Milestone 1 and subsequent milestones. Each program protection plan will include an OPSEC plan or annex. DOD Instruction 5000.2, Defense Acquisition Management Policies and Procedures, requires the integration of OPSEC with security disciplines to protect classified and other sensitive information for each defense acquisition program

b. Nevertheless, PEOs and PMs will use OPSEC to protect critical/sensitive scientific and or technical data in these programs and projects. Many programs and projects involving research do not go past Milestone 1 into further development. Since they do not go before the DAB or ASARC, they may not have program protection plans.

c. PEOs and PMs and other reviewing officials for contracts that are not reviewed by a PM, using defense contracts that require contractor-developed OPSEC plans will ensure that Contract Officer's Technical Representative (COTR) or Contracting Officer's Representative (COR) review the plans prior to their approval. The review of contractor-developed OPSEC plans is a program or project function and not a function of the contracting officer.

d. Contracts that involve unclassified, sensitive information, as defined in 15 USC 278g-3(d)(4), must have either a contractor-developed or a User Agency written OPSEC plan or annex.

2–10. Assistant Secretary of the Army (Research, Development and Acquisition)

The Assistant Secretary of the Army (Research, Development and Acquisition (ASA(RDA)) will—

a. Ensure that program protection plans include OPSEC to protect critical information throughout the life cycle of Army acquisition systems.

b. Ensure that all individuals who perform acquisition duties receive OPSEC training in support of program protection planning.

2–11. Army Chief Information Officer/G-6

The Army Chief Information Officer (CIO)/G-6 will—

a. In coordination with G-2 track and report, on a quarterly basis, open source OPSEC compromises.

b. Ensure that the development and integration of Army C4 systems include OPSEC to protect sensitive and critical information.

c. Plan and implement OPSEC measures throughout the life cycle management of legacy and enterprise systems.

d. Prescribe electromagnetic spectrum and frequency management guidance pertaining to Army OPSEC programs.

e. Prescribe guidance pertaining to evolving voice, data, wireless, and other technologies as they apply to Army OPSEC programs.

2–12. Chief of Public Affairs

The Chief of Public Affairs (CPA) will, in coordination with DCS, G–3/5/7, provide guidance on the release of all information to the public and the media, and ensure that OPSEC has been considered in the preparation of all public releases of information.

2–13. Heads of Army Staff agencies/MACOMs

Heads of Army Staff agencies/MACOMs will designate a point of contact to coordinate OPSEC-related matters with the Army OPSEC program manager. The individual may be a commissioned officer, (CPT or above), warrant officer,(CW2 or above), noncommissioned officer (SFC or above), or a Department of the Army (DA) civilian (grade GS–9 or above).

2–14. Deputy Chief of Staff for Operations and Plans

The Deputy Chief of Staff, G-3/5/7 (DCS, G-3/5/7) will designate a full-time Army OPSEC program manager. This officer will—

a. Coordinate the Army program with the Joint Staff, other Services, DOD agencies, and MACOMs.

b. Represent HQDA on interagency committees, including the National OPSEC Advisory Committee and the National OPSEC Managers Group.

c. Establish Army OPSEC objectives, policies and procedures in AR 530-l consistent with DOD Directive 5205.2, CJCS INST 3213.01, and Joint Pub 3–54.

d. Integrate intelligence, counterintelligence and cover support into OPSEC planning and implementation, with the assistance of the Office of the Deputy Chief of Staff for Intelligence (ODCS, G-2) and other intelligence agencies.

e. Review and evaluate, annually, the Army's OPSEC posture and the effectiveness of MACOM OPSEC programs; provide guidance and assistance as required.

f. Identify resource requirements for the Army OPSEC program.

g. Coordinate with TRADOC for the development of OPSEC doctrine and the integration of OPSEC instruction at Service schools and training centers.

h. Provide evaluations of OPSEC-related material concepts and plans.

i. Establish guidelines for the integration of cover and deception into OPSEC planning and measures.

j. Provide OPSEC planning guidance for operations plans and orders prepared by HQDA and for Army support of JCS directed exercises and operations.

k. Manage Army quotas for attendance at OPSEC training courses conducted by the National Security Agency.

2–15. Deputy Chief of Staff for Intelligence

The Deputy Chief of Staff, G-2 (DCS, G-2) will—

a. Be responsible for Army security policy except for OPSEC and physical security.

b. Assist other Army staff agencies in the development of doctrine and in the preparation of training programs pertinent to all intelligence, counterintelligence and security aspects of OPSEC.

c. Recommend, from an intelligence and security standpoint, the releasability of material and information to foreign governments.

d. Be the Army staff proponent for signal intelligence (SIGINT), human intelligence (HUMINT), imagery intelligence (IMINT) and counterintelligence (CI) activities supporting OPSEC.

e. Incorporate OPSEC policy into AR 380–49.

f. Develop the Army Cover Support Program (AR 381–102 (S)) and provide guidance on the use of cover as an OPSEC protective measure.

2–16. Deputy Chief of Staff, G-1

The Deputy Chief of Staff, G-1 (DCS, G-1) will ensure that personnel actions do not jeopardize the Army's OPSEC posture.

2–17. The Inspector General

The Inspector General (IG) will ensure that OPSEC is an item of interest in inspections of organizations throughout the Army.

2–18. Chief of Engineers

The Chief of Engineers (COE) will—

a. As appropriate, incorporate camouflage and visual deception features in fixed installations and facilities constructed for the Army.

b. As requested and appropriate, incorporate counter surveillance measures in the construction of fixed installations and facilities for the Army.

c. Plan and implement OPSEC measures to protect military construction documents and designs.

d. Coordinate with the Commander, AMC.

(1) Develop and issue design criteria and techniques to provide camouflage and visual deception features in fixed installations and facilities constructed for the Army.

(2) Develop and publish material and design criteria and techniques required to incorporate counter surveillance measures (by others) in fixed installations and facilities constructed for the Army.

(3) Establish a research and development program to produce techniques, materials and design criteria for fixed installations that facilitates camouflage, visual deception, and counter surveillance construction.

e. Provide technical advice on construction related to camouflage and counter surveillance measures.

f. Incorporate OPSEC into appropriate contracts.

2–19. All Army personnel

Operations security is serious business and everyone's responsibility. Failure to properly implement OPSEC procedures can result in serious injury or death to our personnel, damage to key equipment and logistics stockpiles, and/or loss of critical technologies. All Department of the Army personnel (active component, reserve component, DA civilians), and DOD contractors will—

a. Be aware of and support the Army's OPSEC program.

b. Reinforce the vital importance of OPSEC at all times. 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 support activities.

c. Know what their organization considers to be sensitive and critical information.

d. Protect from disclosure any and all sensitive and critical information to which they have personal access.

e. Be aware of the vulnerabilities exposed as a result the disclosure of sensitive and critical information on the Internet. In particular, avoid disclosure of photos showing the results of IED strikes, battle scenes, casualties, destroyed or damaged equipment, enemy KIAs, and access to military facilities.

f. Implement OPSEC measures as prescribed by the Commander or Program Manager (PM).

g. Actively encourage others (including family members and family readiness groups) to protect sensitive and/or critical information.

h. Consult with their immediate supervisor and their OPSEC program manager, prior to publishing or posting information that might contain sensitive and/or critical information in a public forum--this includes, but is not limited to letters, e-mail, Web site postings, Web log (Blog) postings, discussion in internet information forums, discussion in internet message boards, or other forms of dissemination or documentation. Supervisors will advise personnel to ensure that sensitive and critical information are not disclosed. Each unit's OPSEC representative will advise supervisors on means to prevent the disclosure of sensitive and critical information.

i. Handle any attempt by unauthorized personnel to solicit sensitive information, critical information or essential elements of friendly information as a Subversion and Espionage Directed against U.S. Army (SAEDA) incident in accordance with AR 381-12. Report all facts immediately to the nearest supporting counterintelligence office and inform the chain of command. If counterintelligence offices are not readily available, report such incidents to the organizational security manager and to the unit commander.

j. Will not process, store, or transmit information classified above the accreditation level of a DOD computer system. DOD computer systems, including all related equipment, networks and network devices (including Internet access) are provided only for authorized U.S. government use. DOD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes, but is not limited to, active attacks by authorized DOD entities to test or verify the security of the system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over a DOD system may be monitored. Use of a DOD computer system, authorized or unauthorized, constitutes consent to monitoring. Unauthorized use of a DOD computer system may subject the user to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of a DOD computer system constitutes consent for all lawful purposes.

2–20. The Army Operations Security Support Element

The Army OPSEC Support Element (OSE) was established 12 April 2005 under the command and control of Commander, 1st Information Operations Command (Land), FT. Belvoir, VA. which is OPCON to the Army G-3/5/7. The OSE will—

a. Conduct OPSEC assessments/surveys and provide planning support to Army MACOMs, operational units, installations, and programs.

b. Provide OPSEC training and mobile training teams (MTT) in coordination with TRADOC and U.S. Army Space and Missile Defense Command (USASMDC).

c. Support HQDA in the development of OPSEC policy. Support Combined Arms Command (CAC) as the IO Proponent in the development of OPSEC doctrine, training, and tactics, techniques, and procedures (TTP).

d. Support HQDA with the coordination of OPSEC matters affecting intra-service, joint, and DOD components. When tasked by HQDA, represent Army at joint, DOD, and national OPSEC conferences, working groups, and symposiums.

e. Monitor, evaluate, and provide advice to the Army G-3 regarding OPSEC activities.

f. Conduct OPSEC Red Teaming.

2–21. The Army Web Risk Assessment Cell

The Army Web Risk Assessment Cell (AWRAC) is responsible for reviewing the content of Army's publicly accessible Web sites. The AWRAC conducts ongoing operational security and threat assessments of Army Web sites (.mil and all other domains used for communicating official information) to ensure that they are compliant with DOD and Army policies and best practices. The AWRAC will—

a. Conduct random sampling of Web sites to identify security concerns or review Web site concerns provided by the Joint Web Risk Assessment Cell (JWRAC) or Army leadership.

b. Ensure inappropriate sensitive, security and personal information is removed from publicly accessible Web sites.

c. Ensure that Army sites are compliant with other Federal, DOD, and Army Web site administration policies.

d. Notify the Web site owner with operational responsibility and the Information Assurance Program Manager (IAPM) of the respective command/activity of the violations and suspense dates for reporting corrective action.

e. As required, report deficiencies and corrections to the Army CIO/G–6 and JWRAC.

f. Conduct routine checks of Web sites on the world wide web (WWW) for disclosure of sensitive and critical information.

2–22. Office of Judge Advocate General

The Office of the Judge Advocate General (TJAG) will provide legal advice to the Army G-3/5/7, the Army Staff and/or other HQDA activities on OPSEC issues as necessary.

2–23. Public Affairs Officer

Because the Internet is a public forum, Army organizations will ensure that the commander, the public affairs officer (PAO), and other appropriate designee(s) (for example, legal advisor, force protection, intelligence) have properly cleared information posted to the WWW or to the AKO in areas accessible to all account types. Possible risks must be judged and weighed against potential benefits prior to posting any Army information on the WWW. (See para 5–10, AR 25-1.) The designated reviewer(s) will conduct routine reviews of websites on a quarterly basis to ensure that each website is in compliance with the policies of AR 25-1 and that the content remains relevant and appropriate. The minimum review will include all of the website management control checklist items at appendix C, paragraph C–4, AR 25-1. Information contained on publicly accessible websites is subject to the policies and clearance procedures prescribed in AR 360–1, chapter 5, for the release of information to the public. In addition, Army organizations using the WWW will not make the following types of information available on publicly accessible websites:

a. Classified and restricted or limited distribution information.

b. FOUO information.

c. Unclassified information that requires special handling (for example, Encrypt For Transmission Only, Limited Distribution, and scientific and technical information protected under the Technology Transfer Laws).

d. Sensitive information such as proprietary information, predecisional documents, and information that must be protected under legal conditions such as the Privacy Act.

e. FOIA-exempt information. Lists of names and other personally identifying information of personnel assigned within a particular component, unit, organization, or office in the DA are prohibited on the WWW. Discretionary release of names and duty information of personnel who frequently interact with the public by nature of their positions and duties—such as general officers and senior executives, PAOs, or other personnel designated as official command spokespersons—is permitted.

f. Documents or information protected by a copyright.

g. Draft publications.

Chapter 3
Policy and Procedures

Section I
Policy

3–1. General

Operations security applies during peace, crisis, and war to all Army operations and support activities, including RDT&E activities. All Army units, battalion and larger, including equivalent sized TDA organizations, will have OPSEC programs. These programs will use the process described in this chapter to identify and protect critical information.

3–2. Operations Security programs

Commanders and agency heads at battalion and higher echelons will have written OPSEC programs with the following common features:

a. Designation of an OPSEC officer to direct and implement the program. The OPSEC officer can be the operations officer or a subordinate member of that staff element per paragraph 1–7. He may be a commissioned officer, (CPT or above) warrant officer, (CW2 or above) noncommissioned officer (SFC or above) or a civilian (minimum grade GS–9). (See app H for a description of OPSEC officer duties.)

b. 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. Operations security is part of the commanders' initial planning guidance.

c. Use of OPSEC analytic techniques to identify vulnerabilities and to select appropriate OPSEC measures.

d. Training programs to ensure that all personnel, commensurate with their positions and security clearances, are aware of adversary intelligence threats and understand the OPSEC process. Training programs will comply with the requirements in appendix F.

e. Annual review of OPSEC procedures to improve OPSEC programs, include results in annual OPSEC reports up the chain of command. MACOM reports covering the previous fiscal year (1 September to 1 October) are due at HQDA by 1 December. (See app I for the report format.)

f. Provision for cross-command and interagency support and operation on OPSEC programs.

Section II
Procedures

3–3. Operations Security process

Operations security has five steps, which apply to any plan, operation, program, project, or activity. They provide a framework for the systematic process necessary to identify, analyze, and protect information for essential secrecy. The process is continuous. It considers the changing nature of the threat and friendly vulnerabilities throughout the operation. It uses the following steps, but it does not have to follow them in a particular sequence.

a. Identification of critical information.

b. Analysis of threats.

c. Analysis of vulnerabilities.

d. Assessment of risks.

e. Application of appropriate countermeasures (OPSEC measures).

3–4. Identification of critical Information

The purpose of this step is to determine what needs protection. Critical information consists of specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment.

a. Identify key questions that adversary officials and intelligence systems are likely to ask about friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness. These questions are the essential elements of friendly information (EEFI). Answers to EEFI are critical information.

b. There are several sources to help the OPSEC officer formulate these key questions.

(1) The supporting intelligence element can provide information on the adversary and its intelligence requirements. Known tasking of the adversary's intelligence system for answers to specific questions will be part of EEFI.

(2) The next higher echelon publishes EEFI for subordinate units to support its OPSEC program. Most, if not all, of the higher echelon's EEFI will be part of the units' EEFI.

(3) The commander or agency head will provide guidance.

(4) The security classification guide (SCG) for a program or operation identifies classified, critical information. The SCG itself is sensitive information, since it names, by classification level, the most sensitive areas of an activity, program, project, or operation.

(5) Various laws and executive orders require protection of unclassified controlled information.

(a) Information concerning a protected person;

(b) Export controlled technical data (on the Military Critical Technologies List, as required by the Export Administration Act (50 USC App. 2401–2420) of 1979);

(c) Sensitive information (as defined in 15 USC 278g-3(d)(4);

(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; and

(i) Law enforcement information.

(6) Appendix C has sample EEFI by category of 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 the unit's EEFI.

3–5. Analysis of threats

a. The purpose of this step is to identify OPSEC vulnerabilities. Operations security vulnerabilities are 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.

b. In coordination with the intelligence staff, examine each part of the operation to find OPSEC indicators. Compare those indicators with the adversary's intelligence collection capabilities. A vulnerability exists when the adversary can collect an indicator, correctly analyze the information, make a decision, and take timely action to degrade friendly operations. Consider the following questions.

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

(2) What OPSEC indicators will friendly activities create about critical information not already known by the adversary? Operations security indicators are friendly actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. (See app B for sample OPSEC indicators.)

(3) What indicators can the adversary actually collect? This depends on the capabilities of the adversary's intelligence system. (See app E for general characteristics of intelligence systems.)

(4) What indicators will the adversary be able to use to the disadvantage of friendly forces? The answers to this last question are the OPSEC vulnerabilities.

3–6. Analysis of vulnerabilities

The purpose of this step is to identify possible OPSEC measures for each vulnerability. The most desirable measures provide needed protection at the least cost to operational efficiency.

a. Operations security measures are methods and means to gain and maintain essential secrecy about critical information. There are three ways to do this.

(1) Action Control eliminates indicators. Select what actions to undertake, decide whether or not to execute actions, or impose restraints on actions (Specify who, when, where, and how?).

(2) Countermeasures attack the adversary's collection system. Use diversions, camouflage, concealment, jamming, threats, police powers, and force against adversary information gathering and processing capabilities.

(3) Counter analysis provides a possible alternate analysis for an indicator. Confuse the adversary analyst through deception techniques such as covers.

b. Select at least one OPSEC measure for each vulnerability. Some measures may apply to more than one vulnerability.

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. Refer to AR 525–21(C) and FM 90–2 for information on deceptions. Refer to AR 381–102 (S) for information on covers.

e. Appendix G has sample OPSEC measures.

3–7. Assessment of risks

The purpose of this step is to select OPSEC measures for implementation. Only the commander responsible for the mission can make this decision. He must balance the risk of operational failure against the cost of OPSEC measures.

a. Consider the following questions.

(1) What is the likely impact of an OPSEC measure on operational efficiency?

(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?

b. Decide which, if any, OPSEC measures to implement 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.

d. Coordinate OPSEC measures with the other elements of C2W. Their actions can be OPSEC measures.

e. The commander may decide on a no-measures alternative. This is acceptable, if he used the process described herein to determine that no critical information requires protection or that the costs outweigh the risks.

3–8. Application of appropriate countermeasures (operations security measures)

The purpose of this step is to apply OPSEC measures, chosen by the commander, to ongoing activities or to incorporate them into plans for future operations. (Joint and DOD documents label this step as "countermeasures." The Army program uses the same label to keep common terms for joint operations, although this label can be misleading. Joint and DOD publications do recognize countermeasures as a subset of OPSEC measures per paragraph 3–6a of this regulation.)

a. Incorporate OPSEC measures in the operation, activity, acquisition program, or project. Implement 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, state that fact.)

c. Appendix L has the format for an OPSEC annex/appendix/ tab to an OP LAN or OPORD. This format is consistent, as of the date of this regulation, with a draft change to JCS PUB 5–03.2, Joint Operation Planning And Execution System (JOPES), Volume II, Supplemental Planning Formats and Guidance, 10 March 1992.

d. There is no set format for an OPSEC plan. Appendix K has a model outline of an OPSEC plan for activities, programs, or projects not documented by an OPORD or OPLAN. This model can apply to Special Access Programs or Acquisition Systems Program Protection Plans. Tailor the format and content of the OPSEC plan to meet the specific need. As a minimum, address the following points.

(1) Requirements for essential secrecy about friendly intentions and military capabilities from initial planning through postexecution phases.

(2) Tasks to staff and subordinate commands to plan and implement OPSEC measures.

(3) OPSEC estimate comprising identified or assumed adversary knowledge, EEFI, and evaluation of OPSEC effectiveness.

(4) OPSEC threat consisting of detectable activities and the adversary's capability to obtain information.

(5) OPSEC measures to implement.

e. 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.

f. Monitor OPSEC measures during execution. Monitoring is a continuous process of evaluating intelligence and counterintelligence, public media disclosures, signals security (SIGSEC) assessments (including communications security (COMSEC) monitoring), and reports on OPSEC measures. Such reports include OPSEC assessments and surveys (see chap 4).

(1) Evaluate the effectiveness of current OPSEC measures.

(2) Provide emphasis when needed.

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

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

3–9. Planning guidance

a. Operations security steps occur within the military decision making process. The OPSEC officer provides planning guidance for others as they develop their staff estimates. They will identify indicators and vulnerabilities in their functional areas and provide them to the OPSEC officer.

b. OPSEC planning guidance is as detailed as time and available information permit. It includes the following items:

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

(2) Either specific critical information or categories of critical information to protect.

(3) A preliminary list of EEFI.

(4) A summary of adversary intelligence collection capabilities.

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

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

3–10. Lessons learned

Operations security is a continuous requirement. Lessons learned are the basis to improve the OPSEC program. Most lessons arise while monitoring execution of OPSEC measures. Others ensure from an evaluation of a completed operation or program. Prepare lessons learned according to the format in appendix I. Include them with the annual report (see para 3–2e).

Section III
Threat Analysis Support/Protective Measures

3–11. Intelligence threat analysis support to operations security

The intelligence staff of the command will normally provide threat analysis. When this is not practical or possible, forward requirements through channels to the appropriate threat analysis center.

3–12. Information Protection Measures

Careful consideration will be given to classifying and/or applying protective measures, such as For Official Use Only (FOUO), for OPSEC assessments, plans, surveys, EEFI, EPITS, and other OPSEC documentation as appropriate.

Chapter 4
OPSEC Review, Assessment, and Survey

Section I
OPSEC Review

4–1. General

The OPSEC review is an evaluation of a document to ensure protection of sensitive or critical information. The document may be a memorandum, letter, message, briefing, contract, news release, technical document, proposal, plan, order, response to Freedom of information Act (FOIA), or Privacy Act requests or other visual or electronic media. (The OPSEC review of a document is unrelated to the annual program review in para 3–*2e.)*

4–2. Procedures

a. An individual may request an OPSEC review, or the commander may direct one. Standing operating procedures will state which documents automatically go to the OPSEC officer for a review. News releases and responses to FOIA and Privacy Act requests are examples of documents suitable for automatic review.

b. The OPSEC review may take little time or require extensive research over several days. When corrective action is necessary, such as a classification review, the OPSEC officer will provide written recommendations to the appropriate official for immediate action.

c. Technical papers and reports must contain distribution statements according to AR 25–30, AR 70–31, and MIL STD 1806 for contractors producing technical information for the U.S. government.

Section II
Operations Security Assessment

4–3. General

The OPSEC assessment is an analysis of an operation, activity, exercise, or support function to determine the overall OPSEC posture and to evaluate the degree of compliance of subordinate organizations with the published OPSEC plan or OPSEC program.

4–4. Procedures

The organization's OPSEC officer conducts the OPSEC assessment on his own initiative or as the commander directs. He submits a written assessment with results and recommendations to the commander. Contact the local CI office for multi-disciplined CI assistance. An Internal Control Review Checklist will be provided as a guide for an OPSEC assessment.

Section III
Operations Security Survey

4–5. General

The OPSEC survey is a method to determine if there is adequate protection of critical information during planning, preparation, execution, and post-execution phases of any operation or activity. It analyzes all associated functions to identify sources of information, what they disclose, and what can be derived from the information.

a. The objective is to identify OPSEC vulnerabilities in operations or activities, which an adversary could exploit to degrade friendly effectiveness or surprise. The survey helps the commander to monitor OPSEC measures (see para 3–8f) and take further action to maintain essential secrecy.

b. The survey is resource intensive. Conduct an OPSEC assessment first and evaluate its results. Then determine if there is a serious need for an OPSEC survey.

c. The OPSEC survey checks how well a unit executes its plan to protect critical information identified in its EEFI.

(1) Use EEFI, identified in the unit's OPSEC plan, to guide the survey. This is essential, but exercise caution. The unit may not understand EEFI, so it may not have a valid list. The survey team might have to assist the unit to formulate effective EEFI.

(2) When EEFI have not been determined, the surveyed unit's commander must first establish them. Without EEFI, the team cannot determine that actual OPSEC weaknesses exist.

d. The planning, data collection, and analysis functions involved in the survey are common to any analytic effort. An effective survey requires careful prior planning, thorough data collection, and thoughtful analysis of the results. It is essential for survey team members to have experience in the functional areas they will examine. Team members should also have experience in either intelligence or general program analysis.

e. 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 the operation. The examination traces the chronological flow of information from start to finish for each function.

f. OPSEC surveys vary according to the nature of the information, the adversary collection capability, and the environment. In combat, surveys identify weaknesses, which can endanger ongoing and impending combat operations. In peacetime, surveys assist in correcting weaknesses, which disclose information useful to adversaries in future conflict.

g. An OPSEC survey is not an inspection in the traditional sense. There is no grade. A survey is not a check on the effectiveness of a command's security programs or adherence to security directives. Adherence to some security measures can provide indicators of friendly intentions. Overly stringent application of security for classified materials may actually impede operational effectiveness.

(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.

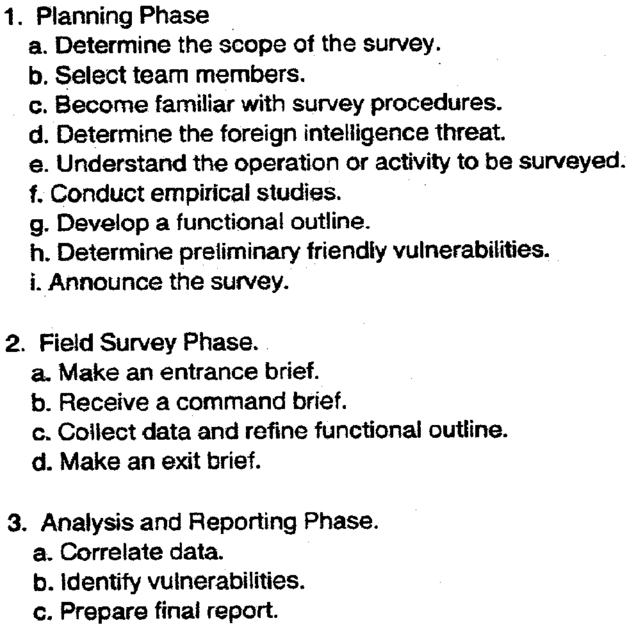
(2) There is no report to the surveyed unit's higher headquarters. As appropriate, the survey team can provide lessons learned without reference to specific units or individuals.

h. There are two types of surveys.

(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 is the focus of the survey. (It crosses command lines with prior coordination.) The survey team includes members from inside and outside the surveyed command. A letter or message initiates the formal survey. It states the subject, team members, and dates of the survey. It can also list commands, activities, and locations.

i. Each survey is unique, as it reflects the operation or activity it analyzes. Nevertheless, there are common procedures, which subsequent paragraphs discuss. (See fig 4–1 for an outline.)



1. Planning Phase
   a. Determine the scope of the survey.
   b. Select team members.
   c. Become familiar with survey procedures.
   d. Determine the foreign intelligence threat.
   e. Understand the operation or activity to be surveyed.
   f. Conduct empirical studies.
   g. Develop a functional outline.
   h. Determine preliminary friendly vulnerabilities.
   i. Announce the survey.

2. Field Survey Phase.
   a. Make an entrance brief.
   b. Receive a command brief.
   c. Collect data and refine functional outline.
   d. Make an exit brief.

3. Analysis and Reporting Phase.
   a. Correlate data.
   b. Identify vulnerabilities.
   c. Prepare final report.

Figure 4–1. OPSEC survey sequence of actions

4–6. Planning phase

Preparation time depends on the nature and complexity of the activities to be surveyed. Allocate sufficient time for thorough document review, coordination, and preparation of functional outlines.

a. Determine the scope of the survey. Define the scope of the survey at the start of the planning phase and keep it manageable. Geography, time, units to be observed, availability of team members, and funding impose limits. Revise the scope at a later date only if significant, new information makes the additional resource investment necessary.

b. Select team members The survey team is multidiscipline. It includes members appropriate to the subject of the survey. Choose the team leader from the operations staff of the commander responsible for the survey. Typical team members represent the functional areas of intelligence, logistics, administration, automated information systems and communications. The survey can require other specialists, such as the leader of a COMSEC monitoring team. Bring team members together early to ensure timely and thorough preparation.

c. Become familiar with survey procedures. The advantages of previous survey experience are obvious, but such personnel may not be available. Familiarize team members with survey techniques, particularly preparation of functional outlines and data collection.

d. Determine the adversary intelligence threat. Evaluate it realistically. Findings for inflated threats, when they are really minimal or nonexistent, diminish the value of the survey. The all-source threat assessment should address the following areas:

(1) Knowledge of adversary intelligence collection activities and interests pertinent to the area concerned.

(2) Possible espionage threats.

(3) Human observation threats.

(4) Open source exploitation threats.

(5) Fixed signals intelligence (SIGINT), acoustic intelligence (ACOUSINT), and radar collection capabilities.

(6) Mobile systems with technical collection capabilities (satellites, surface ships, trucks/vans, submarines, aircraft, and so on.). For each mobile system, list collection capabilities (For example, cameras, radars, SIGINT, and ACOUSINT).

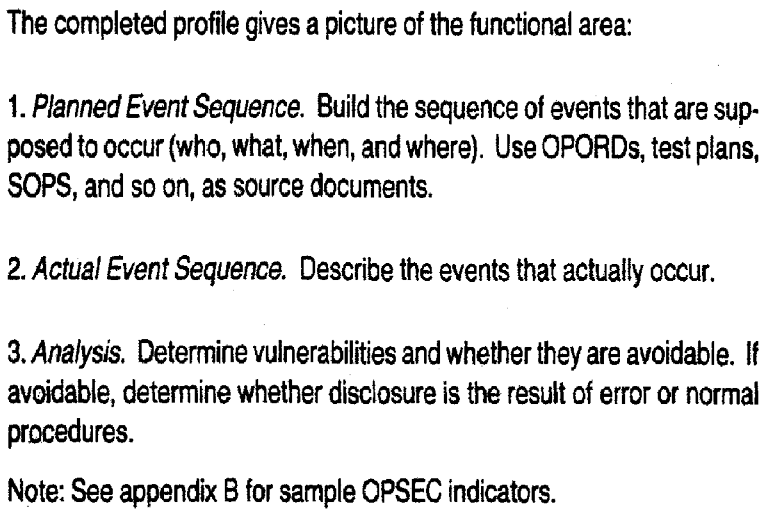
e. Understand the operation or activity to be surveyed. Review OPLANs, OPORDs, standing operating procedures (SOPs), and other directives. Read the OPSEC plan (or annex) and know the EEFI (see para 3–4). Become familiar with the mission, concept of operation, organizational structure, and command relationships. Identify organizations participating in the surveyed activity.

f. Conduct empirical studies. These simulate aspects of the adversary intelligence threat. They support findings or identify vulnerabilities, which the survey team cannot determine through interviews or by observation. Computer modeling and communications monitoring are examples. This requires external support and long lead-time.

g. Develop a functional outline. Construct the chronology of events in the surveyed activity. Describe what, when, and where events occur, and who is involved. Do this for each functional area to include administration, intelligence, operations, logistics, communications and others as appropriate. Use any appropriate format, such as narrative, tabular, or graphic. (See fig 4–2 for a generic functional outline.)

(1) Continue to refine the functional outline during the field survey phase.

(2) Use functional outlines for observations and interviews. For example, group units and facilities geographically to plan the team’s travel itinerary during the field survey phase.



The completed profile gives a picture of the functional area:

1. *Planned Event Sequence.* Build the sequence of events that are supposed to occur (who, what, when, and where). Use OPORDs, test plans, SOPS, and so on, as source documents.

2. *Actual Event Sequence.* Describe the events that actually occur.

3. *Analysis.* Determine vulnerabilities and whether they are avoidable. If avoidable, determine whether disclosure is the result of error or normal procedures.

Note: See appendix B for sample OPSEC indicators.

Figure 4–2. Generic Functional Outline/Profile

h. Determine preliminary friendly vulnerabilities. Use the EEFI, threat, and functional outlines to look for possible vulnerabilities (see para 3–5). Identify indicators, which could enable the adversary to degrade friendly effectiveness. The classified or unclassified nature of the indicator is irrelevant.

i. Announce the survey. The commander of the organizations to be surveyed announces it. Survey will cover the following items:

(1) OPSEC survey purpose and scope.

(2) List of team members and security clearances.

(3) Requirements for briefings and orientations

(4) General time frame of the survey.

(5) Administrative support.

(6) Empirical study support.

4–7. Field survey phase

a. Make an entrance brief. This presentation to the commander and staff of the surveyed organization is either formal or informal. It informs them what the survey will do and how it will be conducted. Cover the purpose and scope of the survey in detail.

(1) Emphasize that the survey is not an inspection, but it is an effort to enhance the ultimate effectiveness of the operation. This briefing lays the groundwork for effective work by, and cooperation with the survey team during the field survey phase.

(2) Summarize the foreign threat and vulnerability assessment developed by the team during the planning phase. Ask the commander and staff to comment on the validity of this assessment.

b. Receive a command brief. The commander and staff of the surveyed unit provide the survey team with an overview of the operation from the command's point of view. Include a tour of the command and control center where feasible. The survey team must resolve any differences between information in the command brief and that determined by the team during the planning phase.

c. Collect data and refine functional outline. Obtain data by observation of activities, document collection, and personnel interviews. Concurrent empirical studies, such as SIGSEC monitoring, also provide data. Be alert to differences between written material, the command brief, interviews, and observations. Expect conflicting data. Determine which information is correct.

(1) Observations verify the occurrence, sequence, and exact timing of events. Interviews provide additional information essential for complete understanding. Record details of how, when, and where personnel accomplish their tasks. Relate these to the planned and observed sequence of events. Obtain copies of documents, which demonstrate potential indicators or vulnerabilities.

(2) Maintain a non-attribution policy regarding sources of information. Interviews are best conducted by two team members. Record the following points:

(a) Identification and purpose of the interview.

(b) Description of the position occupied by the person being interviewed.

(c) Details of how, when, where, and exactly what tasks the individual performs. Determine what information he receives, handles, or generates, and what he does with it.

(d) Awareness of the adversary collection threat in his actions.

(3) Review the functional outline before and after interviews to ensure coverage of all pertinent points. Modify the outline to reflect new information obtained through observations and interviews. Ultimately, each functional outline becomes a profile of actual events. It becomes a chronological record of what happened, where, how, why, and who did it. The outline also has an assessment of the vulnerability of each event to the adversary intelligence threat.

(4) Be familiar with outlines used by other team members. Be alert for information that might affect the other members.

(5) Reassemble the team daily to assess progress, compare data, and coordinate the direction of the survey. This daily discussion generates new investigative directions.

(6) The duration of the field survey phase depends on the rapidity of data collection. Surveys can require thirty or more days in the field. Some factors to consider are:

(a) The proximity of data collection locations to each other.

(b) The total number of data collection points.

(c) Transportation availability.

(d) The degree of difficulty in resolving conflicting data.

(7) As data collection proceeds, tentative findings emerge. When serious, quickly inform the responsible commander to permit early corrective actions. Development of findings while still in the field ensures access to supporting data.

d. Make an exit brief. Brief the commander prior to departure from the area. Provide the major tentative findings of the OPSEC survey.

(1) Emphasize that the findings are tentative and subject to change during detailed analysis and preparation of the survey report. As it may take some time, this exit briefing is an interim basis for corrective action.

(2) Clearly state the distribution of the final report. It is directly to the commander and only to him.

4–8. Analysis and reporting phase

Correlate the data from each refined functional outline and information from empirical studies into one composite operations profile. The operations profile is a complete portrait of the operation. Analyze it to identify vulnerabilities.

a. Correlate empirical data.

(1) Merge all refined functional outlines into one time-phased outline. Describe the sequence of the operation, depict how organizations interact, and trace the flow of information through communications. Portray the information in any manner that facilitates analysis.

(2) Combine empirical data (from para 4–6f) with the time-phased outline to complete the operations profile. When using it, select only data relevant to the operation.

b. Identify vulnerabilities. Look at detectable actions in the operations profile from the adversary’s perspective. Detection alone is not sufficient to have a vulnerability. The adversary must be able to collect, process, and react to detectable actions in sufficient time and manner to degrade friendly effectiveness. Also look for stereotyped or repetitive patterns that are early indicators of friendly intentions.

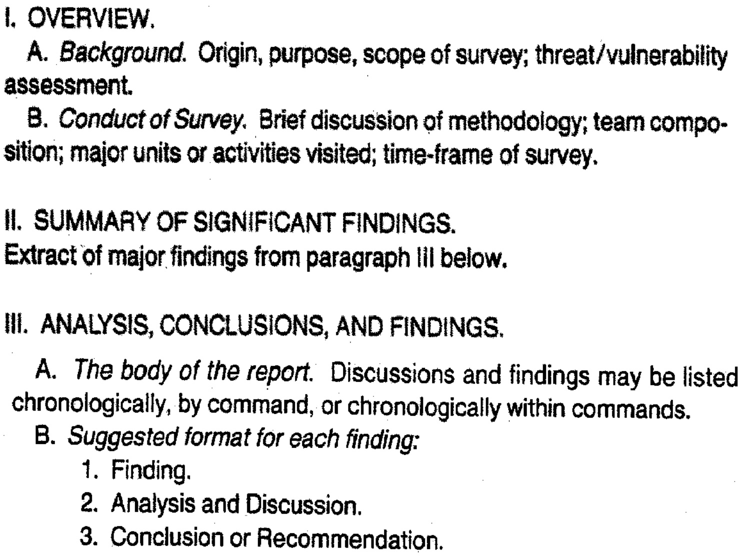
c. Prepare final report. There is no set format for the report. Include an executive summary in lengthy reports. (See fig 4–3.)

(1) Clearly explain and substantiate vulnerabilities or actual sources of detectable indicators. Address all vulnerabilities, even those impossible to eliminate or reduce. This allows the commander to realistically assess the operation.

(2) Limit the length and classification of the threat statement. It only needs to substantiate reported vulnerabilities. Include it either in the main body or as an annex. Concise parts applicable to a particular finding may precede or follow the explanation of the finding.

(3) Introduce each vulnerability with a headline. Follow with a description of the finding. This can include the piece of the operation that entails the vulnerability and the relevant threat. There are several ways to present the vulnerabilities.

(a) In order of significance.
(b) In order of occurrence.
(c) By functional area.
(4) Corrective actions are the prerogative of the surveyed command. The report includes recommendations with the findings. (See para 3–8.)



I. OVERVIEW.

A. *Background.* Origin, purpose, scope of survey; threat/vulnerability assessment.

B. *Conduct of Survey.* Brief discussion of methodology; team composition; major units or activities visited; time-frame of survey.

II. SUMMARY OF SIGNIFICANT FINDINGS.
Extract of major findings from paragraph III below.

III. ANALYSIS, CONCLUSIONS, AND FINDINGS.

A. *The body of the report.* Discussions and findings may be listed chronologically, by command, or chronologically within commands.

B. *Suggested format for each finding:*

1. Finding.
2. Analysis and Discussion.
3. Conclusion or Recommendation.

Figure 4–3. Example OPSEC survey report format

Chapter 5
Special Access Programs

5–1. Overview

a. A Special Access Program (SAP) is a security program established under Executive Order (EO) 12356 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. The controls depend on the criticality of the program and the intelligence threat. The SAP Program Manager, Agency Head, or Commander is responsible for OPSEC for the SAP. Department of the Army SAPs must be approved by the Secretary of the Army and the Deputy Secretary of Defense.

b. AR 380–381(C) prescribes policies and procedures for establishing, administratively controlling, supporting, and disestablishing SAPs.

5–2. Policy

Each SAP will have an OPSEC program from conception to dis-establishment. 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.

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

b. The SAP OPSEC officer will strictly comply with the provisions of chapter 3 of this regulation and AR 380–38l (C). The SAP OPSEC officer is the liaison between the SAP and the command for OPSEC issues. Due to stringent SAP security measures, the command OPSEC officer may not always have knowledge of the SAP.

c. The SAP OPSEC officer will document the SAP's OPSEC program. *Note. See* the format in appendix L (OPSEC annex/app/tab to an OPLAN/ OPORD) or the model outline in appendix K (OPSEC plan).

Chapter 6
OPSEC Contract and Subcontract Requirements

6–1. Overview

Contractors for defense systems acquisition programs will use OPSEC to protect critical information for specific Government contracts and subcontracts. The User Agency/Government Contracting Activity (UA/GCA) imposes OPSEC contractual requirements. It is the responsibility of the UA (that is an Army organization) to determine when OPSEC measures are essential to protect classified or sensitive information for specified contracts.

6–2. Policy and procedures

a. The UA/GCA specifies OPSEC requirements for classified contracts on DD Form 254 (Contract Security Classification Specification). This form defines classification, regarding, downgrading, declassification, and OPSEC specifications for a contract. It applies to classified contracts, and classified subcontracts.

b. The contracting officer or the UA's designated representative is responsible for preparation of the prime contract's DD Form 254. The recipient of the contract will not develop the DD Form 254 on behalf of the UA. Based on the classification guidance and OPSEC requirements in the prime contract, the prime contractor is responsible for preparation of DD Forms 254 for classified subcontracts. This should he done in coordination with the UA OPSEC officer.

c. The UA will state OPSEC requirements on DD Form 254 (and resultant contract or addendum thereto). They will be in sufficient detail to ensure complete contractor understanding of the exact OPSEC provisions or measures required by the UA. Full disclosure of these requirements is essential. Contractors can then comply and charge attendant costs to those contracts. If the OPSEC block is checked on the DD Form 254, the contractor must provide an OPSEC plan to the government.

d. Certain unclassified contracts may require OPSEC. The UA must determine OPSEC requirements when the contract involves sensitive, though unclassified information. When it does, the Contract Data Requirements List (CDRL) and the Statement of Work (SOW) will describe OPSEC requirements.

e. For a contractor to effectively comply with OPSEC provisions of the contract, the UA must provide the following guidance:

(1) Collection Threat documentation.

(2) UA EEFI.

(3) OPSEC plan formats.

(4) OPSEC regulatory documentation.

(5) Specific OPSEC measures that the UA requires (if any).

f. If the UA requires a contractor to adhere to the UA's OPSEC plan, the DD Form 254 will not have OPSEC checked as a requirement. However, the UA must provide the OPSEC plan with the contract data requirements list (CDRL).

g. See DOD 5220.22–M, Industrial Security Manual for Safeguarding Classified Information, for details on OPSEC requirements for Government contracts and subcontracts under the purview of the Defense Investigative Service (DIS). (The National Industrial Security Program Operating Manual (NISPOM), which is currently in draft, will replace DOD 5220.22–M.) "OPSEC requirements, per se, are not part of the Industrial Security Program." They are contract specific and must be added on to the general industrial security requirements stated in the manual for each contract to which they apply. OPSEC requirements should be limited to those requirements that are additional to industrial security requirements stated in the manual. Requirements that are stated in the manual for the protection of classified information should not he repeated as OPSEC requirements. Specific information requiring protection and specific OPSEC requirements must be clearly spelled out to be effective. OPSEC requirements will be inspected by the DIS only if they are mentioned on the DD Form 254 for classified contracts. DIS does not inspect unclassified contractors nor inspect cleared contractors in their performance of unclassified contracts. In those cases, the Contracting officer must designate, if appropriate, a government official to inspect for compliance with OPSEC requirements or otherwise develop a plan for evaluation of compliance.

Appendix A
References

Section I
Required Publications

AR 1–201
Army Inspection Policy. (Cited in para 2–2a.)

AR 380–5
Department of the Army Personnel Security Program (Cited in para 5–1a.)

AR 380–49
Industrial Security Program. (Cited in para 2–15e)

AR 380–381 (C)
Special Access Programs (SAPs) and Sensitive Activities (U). (Cited in paras 5–1b and 5–2b)

AR 381–12
Subversion and Espionage Directed Against U.S. Army (SAEDA). (Cited in para 2–19c.)

AR 525–21 (C)
Battlefield Deception Policy (U). (Cited in 3–6d.)

Section II
Related Publications

A related publication is additional information. The user does not have to read it to understand this publication.

AR 11–7
Internal Review and Audit Compliance Program.

AR 25–1
Army Knowledge Management and Information Technology.

AR 25–2
Information Assurance.

AR 25–55
The Department of the Army Freedom of Information Act Program.

AR 70–1
Army Acquisition Policy.

AR 70–14
Publication and Reprints of Articles in Professional Journals.

AR 70–31
Standards for Technical Reporting.

AR 340–21
The Army Privacy Program.

AR 380–40 (O)
Policy for Safeguarding and Controlling Communication Security (COMSEC) Material (U).

AR 380–53
Information Systems Security Monitoring.

AR 380–67
The Department of the Army Personnel Security Program.

AR 381–10
U.S. Army Intelligence Activities.

AR 381–11
Productions Requirements and Threat Intelligence Support to the U.S. Army.

AR 381–14(S)
Technical Counterintelligence (TCI).

AR 381–20
The U.S. Army Counterintelligence Program.

AR 381–47 (S)
U.S. Army Offensive Counterespionage Operations (U).

AR 381–102 (S)
U.S. Army Cover Program (U).

AR 525–13
Antiterriorism.

AR 525–20
Command and Control Countermeasures (C2CM).

AR 525–22 (S)
Electronic Warfare (EW) Policy (U).

AR 715–30 (C)
Secure Environment Contracting (U).

DOD Acquisitions System Protection Master Plan
DOD Acquisitions System Protection Master Plan.

DODI–5000.2
Operation of the Defense Acquisition System. (Available at http://www.dtic.mil/whs/directives.)

DOD 5105.21–M–1
Department of Defense Sensitive Compartmented Information Administrative Security Manual.

DODD 5205.2
DOD Operations Security (OPSEC) Program. (Available at http://www.dtic.mil/whs.directives.)

DODD 5205.7
Special Access Program (SAP) Policy. (Available at http://www.dtic.mil/whs/directives.)

DOD 5220.22–M
National Industrial Security Program Operating Manual Supplement. (Available at http://www.dtic.mil/whs.directives.)

Joint Pub 1–02
Department of Defense Dictionary of Military and Associated Terms.

Joint Pub 3–13
Joint Doctrine for Information Operations (U).

Joint Pub 3–54
Joint Doctrine for Operations Security.

Joint Pub 5–03.2
Joint Operation Planning and Execution System (JOPES), Volume II, (Planning and Execution Formats and Guidance).

CJCS MOP 6
Electronic Warfare. (Available at http://www.dtic.mil/cjcs_directives.)

CJCS INST 3213.01
Joint Operations Security. (Available at http://www.dtic.mil/cjcs_directives.)

CJCS MOP 30
Command and Control Warfare. (Available at http://www.dtic.mil/cjcs_directives.)

JCS MOP 116
Military Deception. (Available at http://www.jcs.mil.)

JCS MOP 131
Joint and Combined Communications Security. (Available at http://www.jcs.mil.)

Section III
Prescribed Forms

This section contains no entries.

Section IV
Referenced Forms

DD Form 254
Contract Security Classification Specification. (Available at http://www.dtic.mil/whs/directives.)

Appendix B
OPSEC Indicators

B–1. Types

There are three types of indicators.

a. Profile indicators give an analyst patterns and signatures that show how activities are normally conducted.

b. Deviation indicators provide contrasts to normal activity, which help the adversary gain appreciation's about intentions, preparations, time, and place.

c. Tip-off indicators highlight information that otherwise might pass unnoticed. These are most significant when they warn an adversary of impending activity. This allows him to pay closer attention and to task additional collection assets.

B–2. Characteristics

View an indicator's characteristics for its usefulness to the collector on its own and when combined with other indicators. Operations security 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. They minimize 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. They identify how, when, and where the indicator occurs and what pan 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, provide another association. Such continuity can result from repetitive practices or sequencing instead of from planned procedures. When detecting some components of symmetrically arrayed organizations, assume the existence of the rest. For example, suspect the presence of an entire infantry battalion, when intelligence detects only 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 There are other indicators that have not been observed or detected. Each functional activity has a profile of unique indicators, patterns, and associations. The profile of an aircraft deployment, for example, may be unique to the aircraft type or mission. 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 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.

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 in to the background of insignificant anomalies.

B–3. Sample operations security Indicators

The following paragraphs provide a few examples of OPSEC indicators. There are many other indicators 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.

B–4. Administration

a. Temporary duty (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. Notice to airmen (NOTAM) and International Civil Aviation Organization (ICAO) notices.
l. Change of mail addressees or arrangements to forward mail on a large scale.
m. Runs on post exchange for personal articles.
n. Emergency personnel requisitions and fills for critical skills.
o. Emergency recall of personnel on leave and pass.

B–5. Operations, plans, and training

a. Changes in defense readiness condition (DEFCON).
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. Fixed schedules and routes.
h. Standard reactions to hostile acts.
i. Standard maneuvers or procedures.
j. Standard force mixes and numbers to execute particular missions.
k. Changing guards at fixed times.
l. Appearance of special purpose units (bridge companies, path- finders, and so on.).
m. Change in task organization or arrival of new attachments.
n. Artillery registration in new objective area.
o. Surge in fast food (that is, pizza) deliveries to planning staffs at major headquarters.
p. Unit and equipment departures from normal bases.

B–6. Communications

a. Telephone calls among participants in an Operation.
b. Establishment of command nets.
c. Changes in message volume, such as increased radio, teletype, and telephone traffic.
d. Units reporting to new commanders.
e. Identification of units, tasks, or locations in unsecured trans- missions—
f. Increased communications checks.
g. Unnecessary or abnormal reporting.
h. Sudden imposition of COMSEC measures, such as radio listening silence.
i. Appearance of new radio stations in a net.
j. Communications exercises.
k. Appearance of different cryptographic equipment or materials.

B–7. 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’s of friendly units.
k. Friendly unit identifications through COMSEC violation, physical observation of unit symbols, and so forth.
l. Trash that contains unit data.

B–8. 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. POL and ammunition stockpiling.

l. Upgraded lines of communication (LOCS).

m. Delivery of special or uncommon munitions.

n. New support contracts or host nation agreements.

o. Arranging for tugs and harbor pilots.

p. Requisitions in unusual quantities to be filled by a particular date.

B–9. Engineer

a. New facility leases.

b. Construction of mock-ups for special training.

c. Production of unusual numbers of maps and charts for specific locations.

B–10. Medical

a. Stockpiling plasma and medical supplies.

b. Movement of deployable medical sets (DEPMEDS).

B–11. Emissions other than communications

a. Radar and NAVAIDS that reveal location or identity.

b. Normal lighting in a blackout area.

c. Operating at high speed in water.

d. Loud vehicle or personnel movements.

e. Smoke and other odors.

B–12. RDT&E 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 contacts 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 provided insight into the objectives and scope of a system R&D effort 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 manning 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, possesses technology of military significance, or has 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, and so forth) posted where personnel without a need-to-know have access.

o. Conferences, symposia, and internal professional forums

Appendix C
Sample Questions for Essential Elements of Friendly Information (EEFI)

C–1. Courses of Action

What specific courses of action (COAs) are U.S. and allied commands planning?

C–2. Forces

a. What U.S. and allied combat forces are earmarked for possible COAs?

b. What are their levels of readiness?

c. Where are they located?

C–3. Command and Control

a. What are U.S. and allied command arrangements for executing COAs?

b. Where will commanders and command pests be located?

c. What are command post vulnerabilities to attack?

C–4. Communications

a. What are the communications capabilities available for the commander to control and coordinate assigned forces?

b. Where are dedicated communications sites located?

C–5. Logistics

a. What is the logistical posture of U.S. and allied forces?

b. How quickly can ground and air forces he deployed and redeployed?

c. What arc the pertinent ground, air, and sea LOCs, and what are the locations of storage depots, ports, and airfields?

d. What are the vulnerabilities to interdiction of the LOCs?

C–6. Supplies

a. What levels of supplies are available to support combat forces immediately?

b. Where are pre-positioned supplies?

c. How long can combat be sustained with those supplies?

C–7. Locations

a. When will exercises and operations Occur?

b. Where are participating forces located?

C–8. Vulnerabilities

a. What are the defensive dispositions?

b. What sensors and other capabilities are available to detect at- tacks?

c. What vulnerabilities to attack exist?

C–9. Intelligence

a. What are the intelligence, surveillance, and reconnaissance resources available to support the commander?

b. Where are those capabilities located?

c. What operations are being conducted and what are their apparent goals?

d. How can these capabilities be exploited or destroyed?

C–10. Rules of engagement (ROE)

What are the policies and rules of engagement (ROE) that govern the use of weapons and electronic or acoustic warfare systems?

C–11. Allies

a. Which nations will provide support to the U.S.?

b. What vulnerabilities exist that could be exploited to reduce or eliminate such support?

C–12. Maintenance

a. What are the maintenance and salvage capabilities of U.S. and allied forces?

b. To what degree can these capabilities support and sustain forces in combat?

c. What are their vulnerabilities to attack?

C–13. Weapons

a. What are the characteristics and capabilities of weapons and electronic systems available to U.S. and allied forces?

b. What are the doctrines for using various weapons?

c. What are the indicators that nuclear weapons will be employed?

C–14. Psychological operations (PSYOP)

a. What are intended psychological warfare and subversion operations?

b. What are the plans to exploit vulnerabilities?

c. What operations are underway?

d. What U.S. agencies are conducting operations?

C–15. Unconventional Warfare

a. What are intended sabotage and direct action mission targets?

b. What vulnerabilities are planned for exploitation?

c. What capabilities exist to conduct such operations?

d. What U.S. agencies control the resources involved?

C–16. Deception

a. What political and military deceptions are planned?

b. What operations are underway?

c. What U.S. agencies are conducting operations?

C–17. PSYOP Vulnerabilities

What are the vulnerabilities of U.S. forces to psychological warfare and subversion?

C–18. Deception Vulnerabilities

What are the vulnerabilities of U.S. commanders and staffs to deception?

C–19. Political Deception

What are the vulnerabilities of U.S. and allied forces to political deception?

C–20. Counterintelligence

What are U.S. counterintelligence capabilities to detect and neutralize espionage and sabotage nets?

C–21. RDT&E Programs

a. What are the major weapons systems development schedules’?

b. What are the emerging technologies applicable to new weapons systems?

c. What computer software is being used in weapons Systems development, testing and evaluation?

d. What unclassified computer data bases are being used by the RDT&E community?

C–22. Medical

a. What are our causality figures, both actual and projected?

b. Which VIPs are being treated by our Medical Treatment Facilities (MTF)?

c. What is our overall bed/treatment capacity?

d. What increased medical supplies (that is, vaccines, blood products, and so forth) are required by unit or theater?

C–23. Systems Acquisition:

a. What corporations or companies are involved in the acquisition of the system?

b. How much funding does the acquisition program receive?

c. What are the specifics or requirements of the program in acquisition?

d. What are the classification levels of the program?

C–24. Government Contractors

a. In what programs does the contractor provide services and support to the U.S. government?

b. Where are the locations that the contractor performs their work?

c. Is the contractor hiring personnel to work on new or existing contracts or programs?

d. Does the contractor share information or services with other private organizations or companies?

C–25. Arms Control Treaty Inspections

a. What are the missions of the activities on the installations to be visited?

b. Is the installation to be visited self-sufficient or does it rely on the local community for support (that is, telephone service, electricity, water, fire department, police, and so forth)?

c. Are all the buildings on the installation in use, or are only Select facilities utilized?

d. Is the installation an "open post" with unlimited access?

e. What is the morale of all the personnel assigned to the installation? Are there concerns about draw downs, base closures, poor local economy?

f. What is the condition of the installation? Is it run down, well maintained or in need of repair?

g. Are there any portions of the installation that appear to have more protection/security than other parts of the base?

h. What are the security procedures in place at this installation (FBI support, physical security, counterintelligence activities, law enforcement)?

C–26. Special Access Programs

a. What organizations and contractors are involved in the SAP?

b. What is the mission or subject of the SAP?

c. How long will the SAP be operational? What is the current stage of development of the SAP?

d. What are the security procedures for the SAP?

e. What is the budget for the SAP?

C–27. Automated Information Systems (AIS)

a. What measures are taken to prevent unauthorized access to automated information systems (AIS)’s?

b. Are AIS’s approved/certified to process unclassified-sensitive information?

c. Is AIS hardware equipment protected within *an* office environment and/or remote site?

Appendix D
Operations Security Relationships to other Programs

D–1. Background

The U.S. Army has a long history of successful operation's security from the Revolutionary War's Yorktown campaign to OPERATION DESERT STORM. Current OPSEC methodology originated during the Vietnam War. The Purple Dragon Team under U.S. Pacific Command, viewed friendly combat operations from the enemy's perspective. The team used systems analysis to determine what critical information the enemy could learn about friendly operations. The following paragraphs address OPSEC's relationships to other programs.

D–2. Information protection

AR 380–5 provides guidance for classifying material. Protective measures deny unauthorized personnel access to classified material. Both the threat of open source exploitation and procedures intended to keep classified material from appearing in open sources are OPSEC concerns. Bits of information conveyed in non-secure radio transmissions, public releases, briefings for the public, friendly conversations, telephone calls, and so forth, permit hostile intelligence analysts to piece together U.S. intentions and military capabilities. OPSEC prevents critical information (some of which is classified) from appearing in open sources.

D–3. Communications Security

Communications Security (COMSEC) is of particular concern to OPSEC. The intercept of non-secure communications is a significant source of intelligence information for adversaries. Components of COMSEC are cryptographic, transmission, and emissions security.

a. Cryptographic security is classified information transmitted by message or telephone, which is encrypted or sent using an authorized code. OPSEC is concerned with any deviation from established practices that would permit any adversary to "read" U.S. message traffic.

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 communications signals, the intercept of a signal (such as, deviation of location or identity), and the patterns and volumes of communications.

c. Emission security (for example, TEMPEST) is concerned with identifying and eliminating unintentional radiation that conveys classified information.

D–4. Electronic security (ELSEC)

Electronics 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. Another pan involves reducing the information content of the emitters to make them more difficult to identify and locate.

D–5. Physical security

Physical security consists of protective measures to deny unauthorized personnel access to specific areas, facilities, material, or classified information. The implementation of protective measures can reveal vulnerabilities (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). Physical security can be an OPSEC measure.

D–6. Emission control (EMCON)

EMCON encompasses controlling 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 EW.

D–7. Military deception (MD)

MD supports military operations through the application of techniques that simultaneously deny true information or indicators and convey or display false information to adversaries. MD actions mislead adversaries, causing them to derive and accept desired appreciations of U.S. military capabilities, intentions, operations, and other activities. Depending on the objective, MD can be an OPSEC measure, or OPSEC can support MD. When procedural or physical security means are unavailable for controlling OPSEC vulnerabilities, MD can mislead adversaries, thereby minimizing the OPSEC vulnerability.

D–8. Force Protection

Force protection consists of active and passive measures to deter threats directed toward soldiers, their family members, civilians, and the facilities and equipment that supports them. Force Protection uses the planned, integrated, and synchronized application of operations security, combating terrorism, physical security, base defense, personal protective services, law enforcement, and crime prevention. Counterintelligence supports force protection, providing threat information and indicators.

D–9. Computer Security (COMPUSEC)

COMPUSEC prevents the intentional or accidental penetration of Automated Information Systems (AIS). It avoids the disclosure, modification, or destruction of AIS and associated data. Examples are "hacker" penetrations and computer "virus attacks"

D–10. Program Protection Planning (PPP)

The DOD Acquisition Systems Protection Master Plan, dated 12 May 1992, provides a coherent strategy to protect defense technology. It requires PPP for acquisition systems. The PPP uses security disciplines and OPSEC to achieve protection.

Appendix E
The Threat

E–1. Summary

The intelligence threat consists of multiple and overlapping collection efforts targeted against all sources of Army information. Potential adversaries devote significant resources to monitor U.S. military operations and activities on a daily basis. The threat can produce reliable information on the U.S. military establishment and our capabilities, intentions, and vulnerabilities in direct relation to the degree that he is able to collect meaningful information of intelligence value. The threat is also shifting the emphasis in targeting. Foreign targeting of American technology is increasing for economic as well as military reasons. Technology transfer will continue to remain a major concern in the future. The major threat collection disciplines fall in four areas:

a. Human Intelligence (HUMINT).

b. Imagery Intelligence (IMINT).

c. Signals Intelligence (SIGINT).

d. Measurement and Signature Intelligence (MASINT).

E–2. Human Intelligence threat

a. 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, covert, and clandestine operations to achieve worldwide collection objectives.

b. Overt collection operations gather intelligence information from open sources. Vast amounts of information of great interest to foreign intelligence services are readily available. Open sources include newspapers, magazine advertisements; government and trade publications, contract specifications, congressional hearings, computers, and other public media. In excess of 75 percent of the threat's intelligence needs can be satisfied through access to open sources without risk and at minimum cost. Threat HUMINT collectors include official diplomatic and trade representatives, visitors, exchange students, journalists, and military personnel legitimately in the United States.

c. Clandestine collection activities are pursued under cover of business or other activities. Attempts may be made to buy material through third parties or directly as a commercial transaction. Agents may pose as scientists in international projects or symposia, as insurance agents to learn details of a ship's cargo, or as research groups to join international computer nets to obtain data.

d. Clandestine collection operations encompass those activities conducted illegally 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.

(1) 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.

(2) 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.

(3) 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.

E–3. Imagery intelligence threat

Adversaries can obtain IMINT from land, sea, air, and space platforms. The most serious threat at the strategic level stems from photo-reconnaissance 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 enhances the quality and timeliness of the intelligence product for our adversaries.

E–4. Signals intelligence threat

SIGINT incorporates communications intelligence (COMINT) electronics intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT).

a. 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. Major adversaries use various intercept platforms and have a worldwide COMINT capability.

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

c. 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 bio functions or of a ballistic missile's performance.

E–5. Measurement and signature Intelligence threat

MASINT is scientific and technical intelligence obtained by quantitative and qualitative analysis of data derived from technical for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification or measurement. The eight primary disciplines of MASINT are infrared, seismic, radar, laser, effluent, nuclear, optical and unintentional radiation. MASINT includes all technical intelligence except SIGINT and overhead imagery.

E–6. Technology Transfer

The acquisition of sensitive technology by adversaries has led to the significant enhancement of their military-industrial capabilities at the expense of the United States. The Export Administration Act (EAA) of 1979, as amended in 1985 and 1988, addresses this threat by emphasizing the control of critical technology. To accomplish this task, the Department of Defense enacted a series of initiatives to protect U.S. critical technologies. The DOD Acquisition Systems Program implements measures to identify and protect U.S. critical technologies from inception to termination of use. These policies are contained in DOD Directive 5000.1, Defense Acquisition, and DOD Instruction 5000.2, Defense Acquisition Management Policies and Practices. The following serves to outline the threat which 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.

d. 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.

E–7. Non-traditional threats

Past and present allies are potential intelligence adversaries. They can engage in intelligence collection activities to gain economic or political advantages, which are not in the best interest of the U.S.

Appendix F
Training Requirements

F–1. Overview

For Army operations security to be effective, all Army personnel (soldier, civilian, and DOD contractors) must understand how OPSEC complements traditional security programs. All personnel must know how to apply OPSEC to their daily tasks. OPSEC training programs must be action and job-oriented. Use lessons learned to illustrate OPSEC objectives and requirements. Each individual should know the answers to the following questions:

a. What is OP SEC?

b. Why is OPSEC important to my organization?

c. Why is OPSEC important tome?

d. How can I contribute to the OPSEC program?

F–2. Training programs

Commanders will develop OPSEC training programs to accomplish the three categories of training outlined below:

a. Orientation Training. Provide this to all newly assigned personnel within the first 90 days of arrival in the organization. This training will focus on the following areas:

(1) The local, multidiscipline adversary intelligence threat.

(2) How adversaries aggressively seek information on U.S. military capabilities, intentions, and plans.

(3) How OPSEC complements traditional security programs to maintain essential secrecy of U.S. military capabilities, intentions, and plans.

(4) Specific guidance on the EEFI to protect and OPSEC measures to prevent inadvertent disclosure.

b. Awareness training. Provide annual reminders of the importance of sound OPSEC practices needed to deny or control information about organizational capabilities and intentions from foreign intelligence services. This training consists of 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 commanders at commander's calls.

c. OPSEC officer training. Commanders will provide OPSEC officers and other staff personnel with training opportunities that will teach the skills necessary to prepare OPSEC estimates, to prepare OPSEC planning guidance, to plan OPSEC measures, to write OPSEC plans and annexes, and to supervise the execution of OPSEC measures. Funding should be provided in annual training budgets for attendance at OPSEC programs of instruction. OPSEC follow up during and after operations, exercises, and activities assists in the education process and will emphasize the successes and failures of OPSEC measures implemented and specific OPSEC lessons learned.

Appendix G
Sample OPSEC Measures

G–1. Summary

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.

G–2. 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 C2 arrangements.

b. Employ force dispositions and C2 control arrangements that conceal the location, identity, and command relationships of major units.

c. Conduct support activities in away 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 low altitude to avoid radar detection.

f. Operate to minimize the reflective surfaces that units and weapon systems present to radars and sonar's.

g. Use darkness to mask deployments or force generation.

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

G–3. Technical

a. Use radio communications emission control, low probability of intercept techniques, traffic flow security, UHF relay via aircraft, burst transmission technologies, secure phones, landline, and couriers. Limit use of HF radios and directional 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, mountains).

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

e. Use ECM1 camouflage, smoke, background noise, added sources of heat or light, paint, or weather.

G–4. 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 activity.

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

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

G–5. Military Deception

a. Deception can be an effective OPSEC measure, if there is prior coordination when actions will affect other commanders. Use military deception to:

(1) Cause adversary intelligence to fail to target friendly activity; collect against targeted tests, operations, exercises, or other activities; or determine through analysis vital capabilities and characteristics of systems and vital aspects of policies, procedures, doctrine, and tactics.

(2) Create confusion about or multiple interpretations of vital in- formation obtainable from open sources.

(3) Cause loss of interest by foreign and random observers in test, operation, exercise, or other activity.

(4) Convey inaccurate locating and targeting information to op- posing forces.

b. The commander approving an operation or exercise plan has the authority to approve the plan's tactical military deception. An operational commander is authorized to employ tactical military deception measures:

(1) To support OPSEC during the preparation and execution phases of normal operations.

(2) When the commander's forces are engaged or are subject to imminent attack.

G–6. 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 enemy satellites, HF/DF sites, radars, fixed sonar installations, reconnaissance aircraft, and ships.

Appendix H
Standard Duty Description for OPSEC Officers

H–1. Summary

The OPSEC officer administers the commander's OPSEC program. He must know friendly capabilities, intentions and operations that require essential secrecy.

H–2. OPSEC officer duties

a. Policy and management

(1) Interprets OPSEC policies of senior authorities and recommends organizational policies.

(2) Ensures that OPSEC measures conform with guidance from higher authorities.

(3) When appropriate, recommends changes to the policies of higher authorities; and when rules of engagement pertain, requests supplemental rules of engagement in accordance with senior command and CJCS guidance.

(4) Prepares, recommends and supervises execution of the command OPSEC program.

(5) Maintains awareness of all organizational activities that are OPSEC sensitive and advises appropriate personnel about the organization's OPSEC posture and the likelihood that OPSEC can be adequately maintained for those activities.

b. Training.

(1) Supervises organizational OPSEC training, ensuring that assigned personnel are familiar with the significant contribution of the OPSEC process to overall mission effectiveness. Such training should instill an understanding of key OPSEC components that deal with essential secrecy, essential elements of friendly information (EEFI), threat, indicators, and OPSEC measures.

(2) Identifies organizational billets and positions that require specialized OPSEC training, such as planners, inspectors, and contractors. Conducts or schedules required training.

(3) Develops and updates OPSEC awareness training materials for unique organizational activities to supplement standard training materials.

(4) Attends conferences and training sessions, prepares summaries, and provides information to appropriate organizational personnel.

c. Counterintelligence.

(1) Maintains contact with intelligence and security agencies to obtain information that supports the OPSEC planning process.

(2) Prepares requests for all-source intelligence, multidiscipline counterintelligence, and security support for OPSEC planning, surveys, and execution.

(3) Maintains close liaison with counterintelligence personnel in the conduct of operations.

d. Planning and execution.

(1) Coordinates OPSEC planning for future operations and activities.

(2) Prepares organizational OPSEC directives and manuals.

(3) Coordinates the preparation of OPSEC planning guidance for operations and activities.

(4) Assists functional planners in identifying OPSEC indicators, vulnerabilities, and measures.

(5) Supervises implementation of OPSEC measures.

(6) Reviews plans to ensure the adequacy of OPSEC provisions and provides recommendations as appropriate.

(7) Provides OPSEC guidance to command elements involved in developing system requirements and to associated system development, test, and evaluation.

e. Exercises. Supports readiness training and exercises by monitoring and evaluating OPSEC practices and by obtaining outside assistance, as appropriate, to provide realistic simulation of adversary intelligence collection capabilities and techniques.

f. Field Test. Supports field test by—

(1) Assisting in the selection of test field locations.

(2) Providing threat information.

(3) Assisting in the development of

(4) Assisting in the development of OPSEC plans.

(5) Assisting in the development of cover stones and/or concealment.

(6) Providing OPSEC training/briefings prior and subsequent to field test as appropriate.

(7) Performing OPSEC reviews of test reports/results/activities prior to public release.

(8) Conducting OPSEC assessments/surveys of tests as appropriate.

g. OPSEC surveys

(1) Identifies requirements for OPSEC surveys, funding for surveys, coordinates survey scheduling, and arranges survey team augmentation from other sources as required.

(2) Prepares OPSEC survey directives and coordinates or conducts the survey.

(3) Participates in survey debriefings and arranges with the commander for releasing lessons learned to other organizations.

h. Administration.

(1) Prepares an annual OPSEC report per appendix I.

(2) Prepares OPSEC lessons learned per paragraph 3–10.

H–3. Qualifications

a. Experience.

(1) Operations experience is essential to the OPSEC officer.

(2) The OPSEC officer should be experienced in planning and conducting information gathering activities, processing and extracting data from materials gathered, the concept of indications and warnings, and problem-solving techniques. Ideally, the OPSEC officer would have experience in the intelligence process, including intelligence analysis and estimation techniques. This experience is secondary to operations experience.

b. Knowledge.

(1) Thorough comprehension of the functional relationships and procedural processes of the command or organization.

(2) Working knowledge of Army and command planning systems, directives, and major war plans.

(3) Thorough understanding of OPSEC concepts, procedures, and policies.

(4) Understanding of technical countermeasures, military deception, and counterintelligence operations to support OPSEC planning.

(5) Understanding of U.S. intelligence and counterintelligence organizations and how to obtain support from them.

(6) Basic knowledge of traditional security programs intended to protect classified information and matters, and their distinct relationship to OPSEC.

c. OPSEC skills.

(1) Ability to evaluate competitive situations and to prepare various types of OPSEC plans.

(2) Ability to prepare plans for various types of OPSEC measures, including covers, diversions, other military deceptions, countermeasures, and the use of force.

(3) Ability to provide advice about policies, doctrines, and guidance and apply effective OPSEC measures.

(4) Ability to integrate and coordinate OPSEC planning with the other elements of C2W

d. Communicative skills.

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

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

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

(4) Ability to work with professionals and specialists to communicate requirements and to obtain accurate information pertaining to OPSEC planning.

e. Security clearance.

(1) OPSEC officers will be granted a TOP SECRET clearance and access to sensitive compartmented information (SCI) when appropriate.

(2) The organization will ensure that an SCI billet is available for the OPSEC officer when appropriate.

Appendix I
Annual OPSEC Report Format

I–1. Overview of OPSEC Program Status

Provide a summary of the overall condition of the OPSEC program. Highlight key successes and problems that will be discussed in greater detail in other portions of the report. The reporting period is from 1 October to 30 September (that is, the prior fiscal year). Reports from MACOMs are due at HQDA by 1 December each year.

I–2. OPSEC Plans and Activities Conducted During the Reporting Period

a. Focus on how the organization applied the process. Avoid emphasizing traditional security measures (for example, telephone monitoring, procuring secure telephones, or improving access control to sensitive areas), except to the extent were used to eliminate or reduce identified OPSEC vulnerabilities.

b. Appropriate activities for this portion of the report might include—

(1) Writing an OPLAN Annex L on OPSEC.

(2) Providing OPSEC support for the planning and execution of real-world contingency operations, exercises, RDT&E activities, and so on.

(3) Conducting OPSEC surveys for the above-mentioned activities.

(4) Implementing OPSEC measures to protect identified vulnerabilities.

(5) Creating, operating, and providing findings of organizational OPSEC advisory bodies and hoards.

(6) Training initiatives or improvements for OPSEC.

I–3. Miscellaneous Problems and Recommendations

Address problems, not necessarily related to subjects in paragraph I–2 above, that impact on the command's overall OPSEC posture. Such problems might include, personnel manning or administrative problems.

I–4. Forecast of OPSEC Activities and Objectives for the Next Reporting Period

Address those planned actions that will improve the OPSEC posture of the command. These actions could involve new initiatives or refinement of OPSEC activities reported in paragraph I–2.

I–5. Lessons Learned

a. The lesson learned should be a case study that portrays specific problems or successes identified in OPSEC surveys, exercises, RDT&E activities, contingency operations, arms control treaty inspections, or other activities. Each lesson learned must stand alone to achieve maximum effectiveness as a training tool or planning input.

b. Each lesson learned case study will be consistent with formats used in the Joint Universal Lessons Learned System as follows:

(1) *Title.* Should reflect both the subject area and the nature of the problem (for example, Deployment Procedures for Contingency Corps Units).

(2) *Observation* Concisely state the problem.

(3) *Discussion* This is the heart of the lesson-learned case study. Provide perspective by answering who, what, where, when, why, and how about the problem. If the problem could not be solved, explain why.

(4) *Lesson-Learned.* State what positive action was taken, or should have been taken, to avoid or alleviate the problem. Avoid restating or paraphrasing the problem. Concentrate on the positive action.

(5) *Recommended Action.* State how to permanently correct the problem. If no corrective action is necessary, enter "None required."

(6) *Comments.* Provide other information that does not fit any previous category. Indicate here if non-attribution is desired.

I–6. OPSEC Point of Contact

a. Name.

b. Complete mailing address.

c. DSN phone number.

d. Secure phone number.

e. Electronic message address.

Appendix J
Annual Army OPSEC Achievement Awards Program

J–1. Purpose

The Army OPSEC Achievement Awards Program recognizes significant accomplishments by organizations and individuals in operations security.

J–2. Scope

a. These non-monetary awards cover the period from 1 October through 30 September each Year.

b. The organizational award is for any size unit. Both MTOE and TDA units are eligible.

c. The individual award is for any individual, military or civilian, in any grade, belonging to any organization.

d. Each Army major command may submit one nominee in each of the two categories.

J–3. Nomination Criteria

a. Examples of significant accomplishments for organizational achievement awards:

(1) Establishment of a viable OPSEC program within the organization or unit.

(2) Identification or solution of significant OPSEC problems.

(3) Innovative or improved awareness, education, and training objectives.

(4) Identification of significant threats or vulnerabilities.

(5) Identification of significant measures to eliminate or reduce threats or vulnerabilities.

(6) The emphasis should be on an achievement that leads to an improvement in the organization's effectiveness through implementation of an OPSEC program or practices.

b. Examples of significant accomplishments for individual achievement awards:

(1) Nominees should have made a significant contribution in the field of OPSEC that reflects creative or innovative application of techniques or methods to solve problems related to OPSEC.

(2) The achievement or contribution should be creative, of outstanding professional caliber, and should add to the general store of OPSEC methods and techniques.

(3) The achievement should lead to an improvement in the Army or organizational OPSEC posture.

(4) Nominees should have demonstrated personal leadership in application of OPSEC policy or doctrine.

(5) Nominees may have been involved in an initiative leading to improvements or measures to reduce specific OPSEC threats or vulnerabilities.

(6) Contributions to the identification of or solution to significant OPSEC problems should be considered. The achievement may be the identification of significant threats or vulnerabilities.

(7) Contributions to innovative or improvised awareness, education, and training initiatives are to be considered. This also applies to the study of OPSEC lessons learned to improve the organization.

J–4. Submission Requirements

Prepare nominations according to the following guidance:

a. Identification of the nominated organization or individual and locations of the nominees.

b. A narrative, not to exceed two pages in length, describing the specific OPSEC accomplishments of the organization or individual nominated. Written material shall not exceed the SECRET level.

c. A short biography of the individual nominated for the individual achievement award.

d. The name and telephone number of a person, knowledgeable about the material submitted, who can provide additional information if needed. Nominations from MACOMs are due at HQDA (DAMO-ODL–CHT) not later than 15 December.

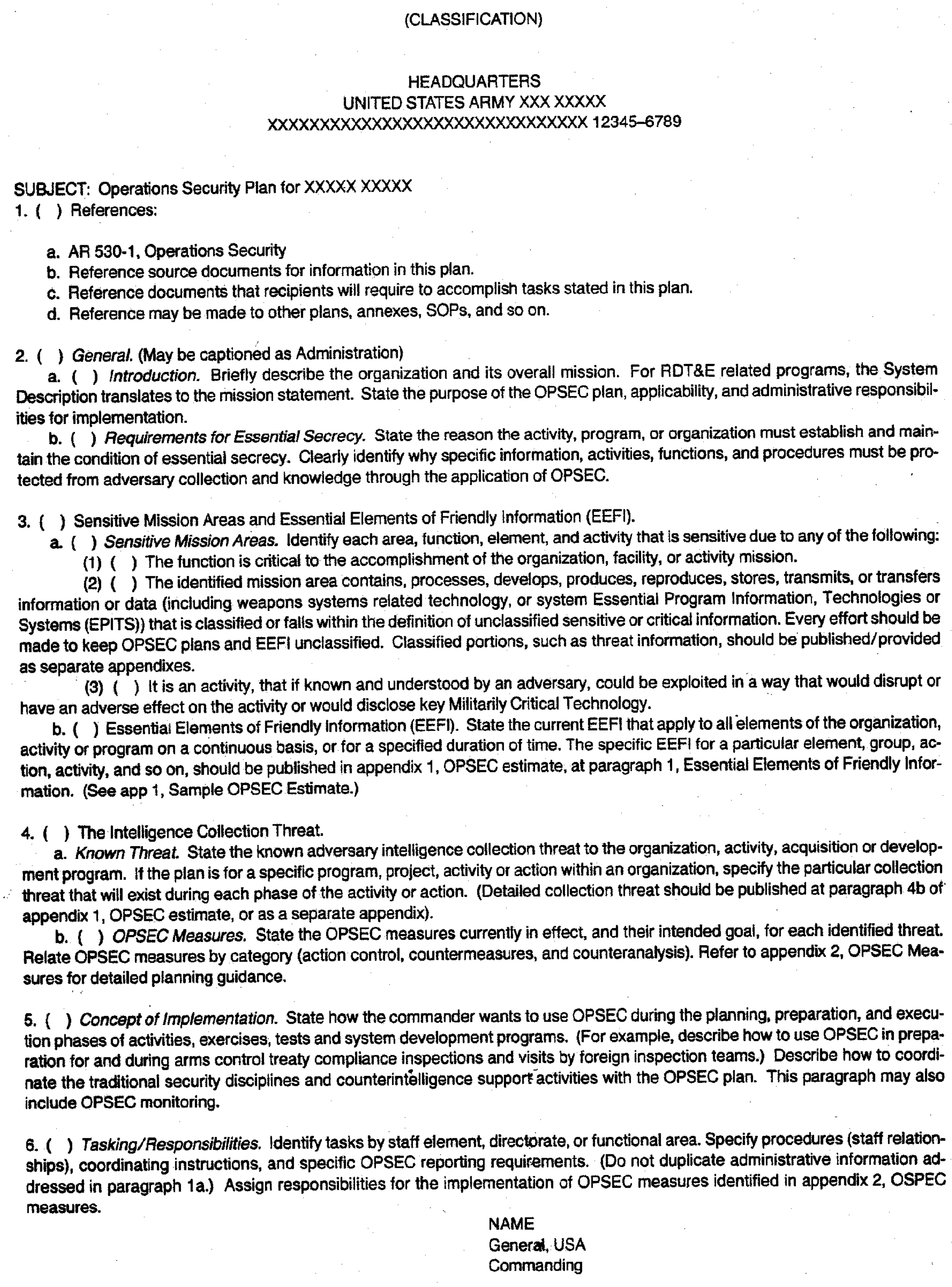
J–5. Recognition

a. HQDA will select 'winners in both categories by 31 January of the next year.

b. Winners will be the Department of the Army's nominees for the National OPSEC Achievement Awards Program at the Federal Government level.

Appendix K
Model Outline for an OPSEC Plan

Use this outline as a guide when writing an OPSEC plan for activities, programs, or projects not documented by an OPORD or OPLAN. This model applies to the Acquisition Systems Protection Program and Special Access Programs (SAPs).



(CLASSIFICATION)

HEADQUARTERS
UNITED STATES ARMY XXX XXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX 12345–6789

SUBJECT: Operations Security Plan for XXXXX XXXXX

1. ( ) References:

a. AR 530-1, Operations Security
b. Reference source documents for information in this plan.
c. Reference documents that recipients will require to accomplish tasks stated in this plan.
d. Reference may be made to other plans, annexes, SOPs, and so on.

2. ( ) *General.* (May be captioned as Administration)

a. ( ) *Introduction.* Briefly describe the organization and its overall mission. For RDT&E related programs, the System Description translates to the mission statement. State the purpose of the OPSEC plan, applicability, and administrative responsibilities for implementation.

b. ( ) *Requirements for Essential Secrecy.* State the reason the activity, program, or organization must establish and maintain the condition of essential secrecy. Clearly identify why specific information, activities, functions, and procedures must be protected from adversary collection and knowledge through the application of OPSEC.

3. ( ) Sensitive Mission Areas and Essential Elements of Friendly Information (EEFI).

a. ( ) *Sensitive Mission Areas.* Identify each area, function, element, and activity that is sensitive due to any of the following:

(1) ( ) The function is critical to the accomplishment of the organization, facility, or activity mission.

(2) ( ) The identified mission area contains, processes, develops, produces, reproduces, stores, transmits, or transfers information or data (including weapons systems related technology, or system Essential Program Information, Technologies or Systems (EPITS)) that is classified or falls within the definition of unclassified sensitive or critical information. Every effort should be made to keep OPSEC plans and EEFI unclassified. Classified portions, such as threat information, should be published/provided as separate appendixes.

(3) ( ) It is an activity, that if known and understood by an adversary, could be exploited in a way that would disrupt or have an adverse effect on the activity or would disclose key Militarily Critical Technology.

b. ( ) Essential Elements of Friendly Information (EEFI). State the current EEFI that apply to all elements of the organization, activity or program on a continuous basis, or for a specified duration of time. The specific EEFI for a particular element, group, action, activity, and so on, should be published in appendix 1, OPSEC estimate, at paragraph 1, Essential Elements of Friendly Information. (See app 1, Sample OPSEC Estimate.)

4. ( ) The Intelligence Collection Threat.

a. *Known Threat.* State the known adversary intelligence collection threat to the organization, activity, acquisition or development program. If the plan is for a specific program, project, activity or action within an organization, specify the particular collection threat that will exist during each phase of the activity or action. (Detailed collection threat should be published at paragraph 4b of appendix 1, OPSEC estimate, or as a separate appendix).

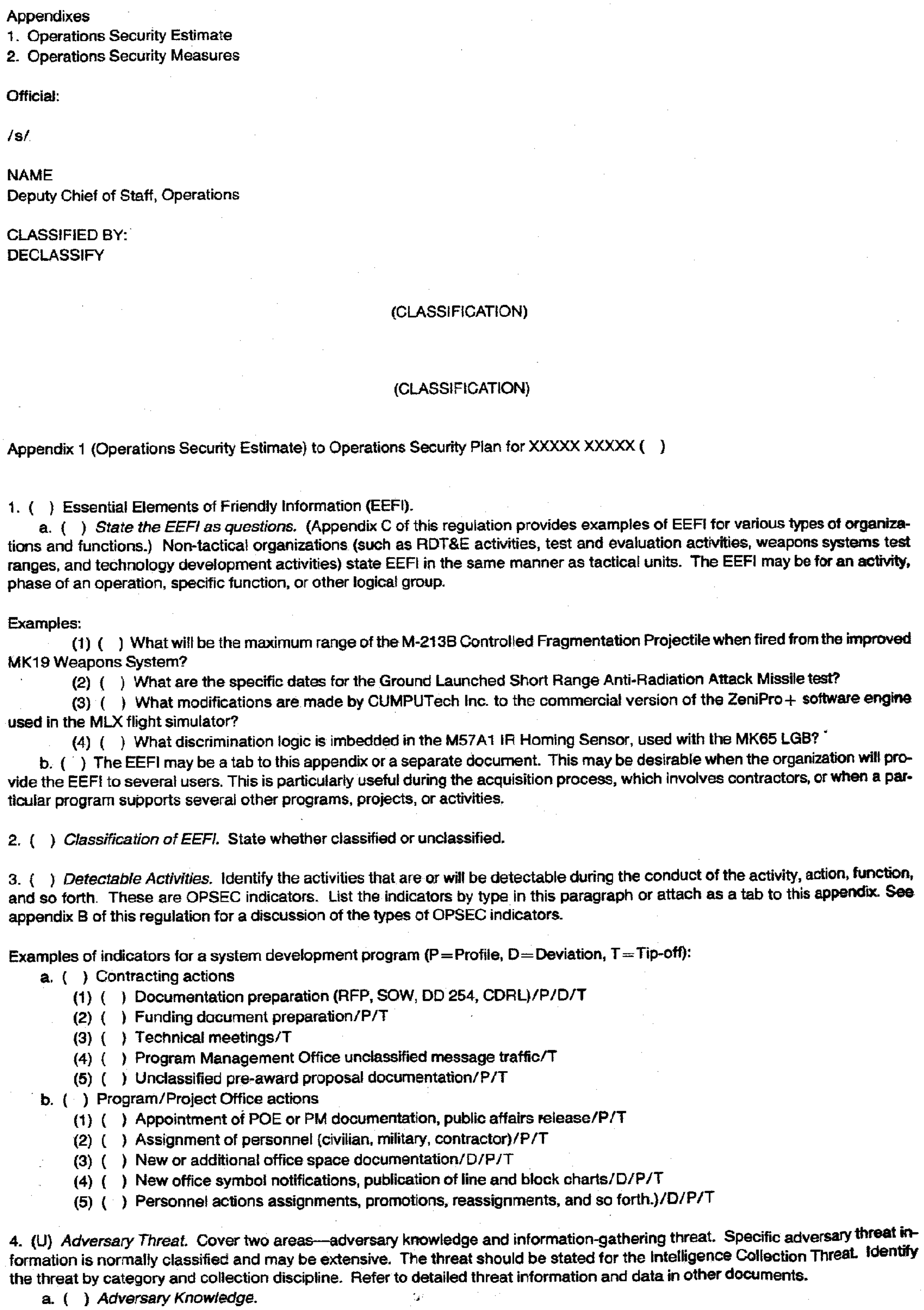
b. ( ) *OPSEC Measures.* State the OPSEC measures currently in effect, and their intended goal, for each identified threat. Relate OPSEC measures by category (action control, countermeasures, and counteranalysis). Refer to appendix 2, OPSEC Measures for detailed planning guidance.

5. ( ) *Concept of Implementation.* State how the commander wants to use OPSEC during the planning, preparation, and execution phases of activities, exercises, tests and system development programs. (For example, describe how to use OPSEC in preparation for and during arms control treaty compliance inspections and visits by foreign inspection teams.) Describe how to coordinate the traditional security disciplines and counterintelligence support activities with the OPSEC plan. This paragraph may also include OPSEC monitoring.

6. ( ) *Tasking/Responsibilities.* Identify tasks by staff element, directorate, or functional area. Specify procedures (staff relationships), coordinating instructions, and specific OPSEC reporting requirements. (Do not duplicate administrative information addressed in paragraph 1a.) Assign responsibilities for the implementation of OPSEC measures identified in appendix 2, OSPEC measures.

NAME
General, USA
Commanding

Figure K–1. Sample outline for writing an OPSEC plan-continued



Appendixes
1. Operations Security Estimate
2. Operations Security Measures

Official:

/s/

NAME
Deputy Chief of Staff, Operations

CLASSIFIED BY:
DECLASSIFY

(CLASSIFICATION)

(CLASSIFICATION)

Appendix 1 (Operations Security Estimate) to Operations Security Plan for XXXXX XXXXX ( )

1. ( ) Essential Elements of Friendly Information (EEFI).

a. ( ) *State the EEFI as questions.* (Appendix C of this regulation provides examples of EEFI for various types of organizations and functions.) Non-tactical organizations (such as RDT&E activities, test and evaluation activities, weapons systems test ranges, and technology development activities) state EEFI in the same manner as tactical units. The EEFI may be for an activity, phase of an operation, specific function, or other logical group.

Examples:

(1) ( ) What will be the maximum range of the M-213B Controlled Fragmentation Projectile when fired from the improved MK19 Weapons System?

(2) ( ) What are the specific dates for the Ground Launched Short Range Anti-Radiation Attack Missile test?

(3) ( ) What modifications are made by CUMPUTech Inc. to the commercial version of the ZeniPro+ software engine used in the MLX flight simulator?

(4) ( ) What discrimination logic is imbedded in the M57A1 IR Homing Sensor, used with the MK65 LGB?

b. ( ) The EEFI may be a tab to this appendix or a separate document. This may be desirable when the organization will provide the EEFI to several users. This is particularly useful during the acquisition process, which involves contractors, or when a particular program supports several other programs, projects, or activities.

2. ( ) *Classification of EEFI.* State whether classified or unclassified.

3. ( ) *Detectable Activities.* Identify the activities that are or will be detectable during the conduct of the activity, action, function, and so forth. These are OPSEC indicators. List the indicators by type in this paragraph or attach as a tab to this appendix. See appendix B of this regulation for a discussion of the types of OPSEC indicators.

Examples of indicators for a system development program (P=Profile, D=Deviation, T=Tip-off):

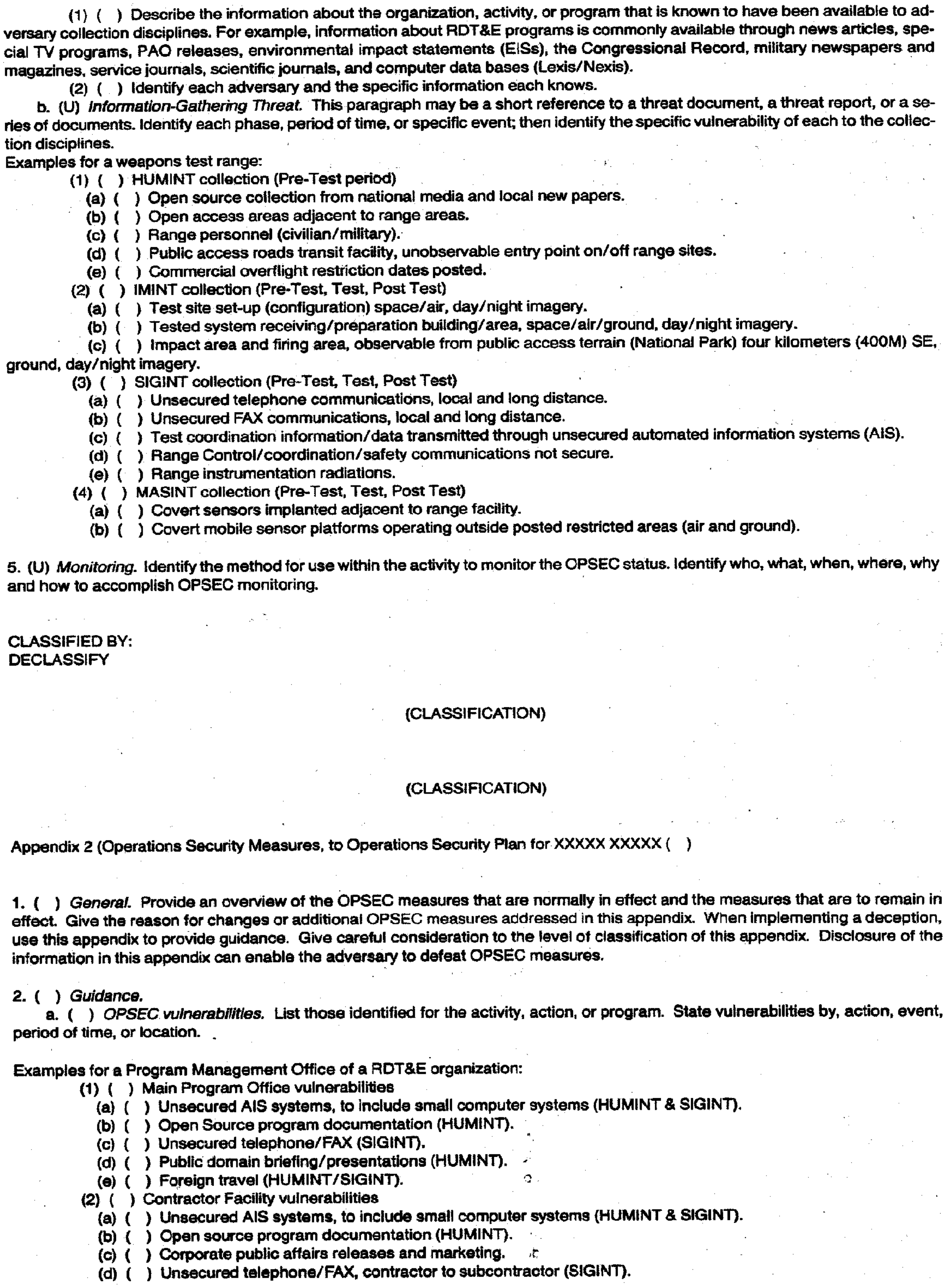
a. ( ) Contracting actions
(1) ( ) Documentation preparation (RFP, SOW, DD 254, CDRL)/P/D/T
(2) ( ) Funding document preparation/P/T
(3) ( ) Technical meetings/T
(4) ( ) Program Management Office unclassified message traffic/T
(5) ( ) Unclassified pre-award proposal documentation/P/T

b. ( ) Program/Project Office actions
(1) ( ) Appointment of POE or PM documentation, public affairs release/P/T
(2) ( ) Assignment of personnel (civilian, military, contractor)/P/T
(3) ( ) New or additional office space documentation/D/P/T
(4) ( ) New office symbol notifications, publication of line and block charts/D/P/T
(5) ( ) Personnel actions assignments, promotions, reassignments, and so forth.)/D/P/T

4. (U) *Adversary Threat.* Cover two areas—adversary knowledge and information-gathering threat. Specific adversary threat information is normally classified and may be extensive. The threat should be stated for the Intelligence Collection Threat. Identify the threat by category and collection discipline. Refer to detailed threat information and data in other documents.

a. ( ) *Adversary Knowledge.*

Figure K–1. Sample outline for writing an OPSEC plan-continued



(1) ( ) Describe the information about the organization, activity, or program that is known to have been available to adversary collection disciplines. For example, information about RDT&E programs is commonly available through news articles, special TV programs, PAO releases, environmental impact statements (EISs), the Congressional Record, military newspapers and magazines, service journals, scientific journals, and computer data bases (Lexis/Nexis).

(2) ( ) Identify each adversary and the specific information each knows.

b. (U) *Information-Gathering Threat.* This paragraph may be a short reference to a threat document, a threat report, or a series of documents. Identify each phase, period of time, or specific event; then identify the specific vulnerability of each to the collection disciplines.

Examples for a weapons test range:

(1) ( ) HUMINT collection (Pre-Test period)
(a) ( ) Open source collection from national media and local new papers.
(b) ( ) Open access areas adjacent to range areas.
(c) ( ) Range personnel (civilian/military).
(d) ( ) Public access roads transit facility, unobservable entry point on/off range sites.
(e) ( ) Commercial overflight restriction dates posted.
(2) ( ) IMINT collection (Pre-Test, Test, Post Test)
(a) ( ) Test site set-up (configuration) space/air, day/night imagery.
(b) ( ) Tested system receiving/preparation building/area, space/air/ground, day/night imagery.
(c) ( ) Impact area and firing area, observable from public access terrain (National Park) four kilometers (400M) SE, ground, day/night imagery.
(3) ( ) SIGINT collection (Pre-Test, Test, Post Test)
(a) ( ) Unsecured telephone communications, local and long distance.
(b) ( ) Unsecured FAX communications, local and long distance.
(c) ( ) Test coordination information/data transmitted through unsecured automated information systems (AIS).
(d) ( ) Range Control/coordination/safety communications not secure.
(e) ( ) Range instrumentation radiations.
(4) ( ) MASINT collection (Pre-Test, Test, Post Test)
(a) ( ) Covert sensors implanted adjacent to range facility.
(b) ( ) Covert mobile sensor platforms operating outside posted restricted areas (air and ground).

5. (U) *Monitoring.* Identify the method for use within the activity to monitor the OPSEC status. Identify who, what, when, where, why and how to accomplish OPSEC monitoring.

CLASSIFIED BY:
DECLASSIFY

(CLASSIFICATION)

(CLASSIFICATION)

Appendix 2 (Operations Security Measures, to Operations Security Plan for XXXXX XXXXX ( )

1. ( ) *General.* Provide an overview of the OPSEC measures that are normally in effect and the measures that are to remain in effect. Give the reason for changes or additional OPSEC measures addressed in this appendix. When implementing a deception, use this appendix to provide guidance. Give careful consideration to the level of classification of this appendix. Disclosure of the information in this appendix can enable the adversary to defeat OPSEC measures.

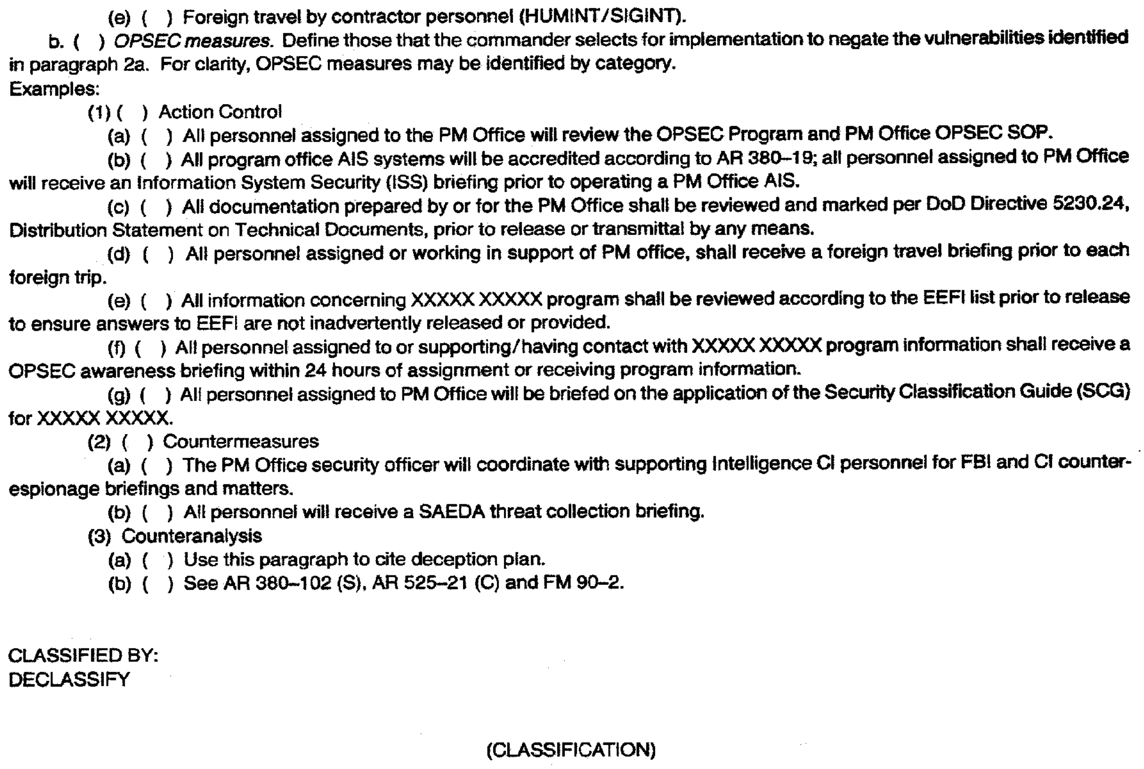
2. ( ) *Guidance.*

a. ( ) *OPSEC vulnerabilities.* List those identified for the activity, action, or program. State vulnerabilities by, action, event, period of time, or location.

Examples for a Program Management Office of a RDT&E organization:

(1) ( ) Main Program Office vulnerabilities
(a) ( ) Unsecured AIS systems, to include small computer systems (HUMINT & SIGINT).
(b) ( ) Open Source program documentation (HUMINT).
(c) ( ) Unsecured telephone/FAX (SIGINT).
(d) ( ) Public domain briefing/presentations (HUMINT).
(e) ( ) Foreign travel (HUMINT/SIGINT).
(2) ( ) Contractor Facility vulnerabilities
(a) ( ) Unsecured AIS systems, to include small computer systems (HUMINT & SIGINT).
(b) ( ) Open source program documentation (HUMINT).
(c) ( ) Corporate public affairs releases and marketing.
(d) ( ) Unsecured telephone/FAX, contractor to subcontractor (SIGINT).

Figure K–1. Sample outline for writing an OPSEC plan-continued



(e) ( ) Foreign travel by contractor personnel (HUMINT/SIGINT).

b. ( ) *OPSEC measures.* Define those that the commander selects for implementation to negate the vulnerabilities identified in paragraph 2a. For clarity, OPSEC measures may be identified by category.

Examples:

(1) ( ) Action Control

(a) ( ) All personnel assigned to the PM Office will review the OPSEC Program and PM Office OPSEC SOP.

(b) ( ) All program office AIS systems will be accredited according to AR 380–19; all personnel assigned to PM Office will receive an Information System Security (ISS) briefing prior to operating a PM Office AIS.

(c) ( ) All documentation prepared by or for the PM Office shall be reviewed and marked per DoD Directive 5230.24, Distribution Statement on Technical Documents, prior to release or transmittal by any means.

(d) ( ) All personnel assigned or working in support of PM office, shall receive a foreign travel briefing prior to each foreign trip.

(e) ( ) All information concerning XXXXX XXXXX program shall be reviewed according to the EEFI list prior to release to ensure answers to EEFI are not inadvertently released or provided.

(f) ( ) All personnel assigned to or supporting/having contact with XXXXX XXXXX program information shall receive a OPSEC awareness briefing within 24 hours of assignment or receiving program information.

(g) ( ) All personnel assigned to PM Office will be briefed on the application of the Security Classification Guide (SCG) for XXXXX XXXXX.

(2) ( ) Countermeasures

(a) ( ) The PM Office security officer will coordinate with supporting Intelligence CI personnel for FBI and CI counterespionage briefings and matters.

(b) ( ) All personnel will receive a SAEDA threat collection briefing.

(3) Counteranalysis

(a) ( ) Use this paragraph to cite deception plan.

(b) ( ) See AR 380–102 (S), AR 525–21 (C) and FM 90–2.

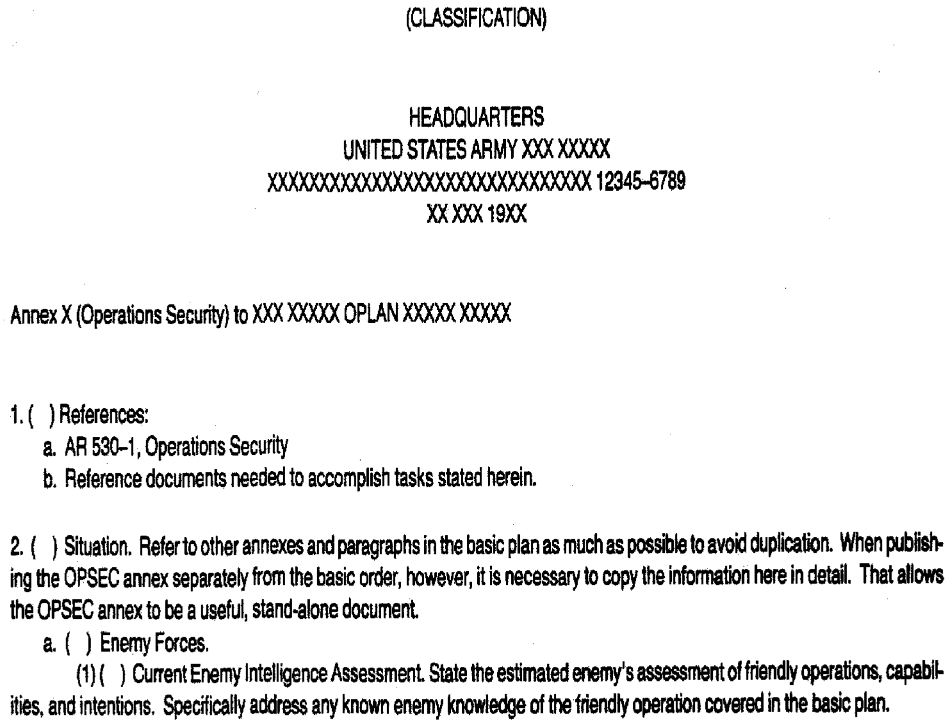
CLASSIFIED BY:
DECLASSIFY

(CLASSIFICATION)

Figure K–1. Sample outline for writing an OPSEC plan

Appendix L
Format for OPSEC Annex/Appendix/Tab to OPLANI OPORD

Use the following format to cover OPSEC in an OPLAN or OPORD. It is valid no matter how the OPLAN or OPORD is organized. (It can include OPSEC in an annex, an appendix to an annex, or a tab to an appendix to an annex.) The format and contents of the five paragraphs and their subparagraphs remain the same.



(CLASSIFICATION)

HEADQUARTERS
UNITED STATES ARMY XXX XXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX 12345-6789
XX XXX 19XX

Annex X (Operations Security) to XXX XXXXX OPLAN XXXXX XXXXX

1. ( ) References:

a. AR 530-1, Operations Security

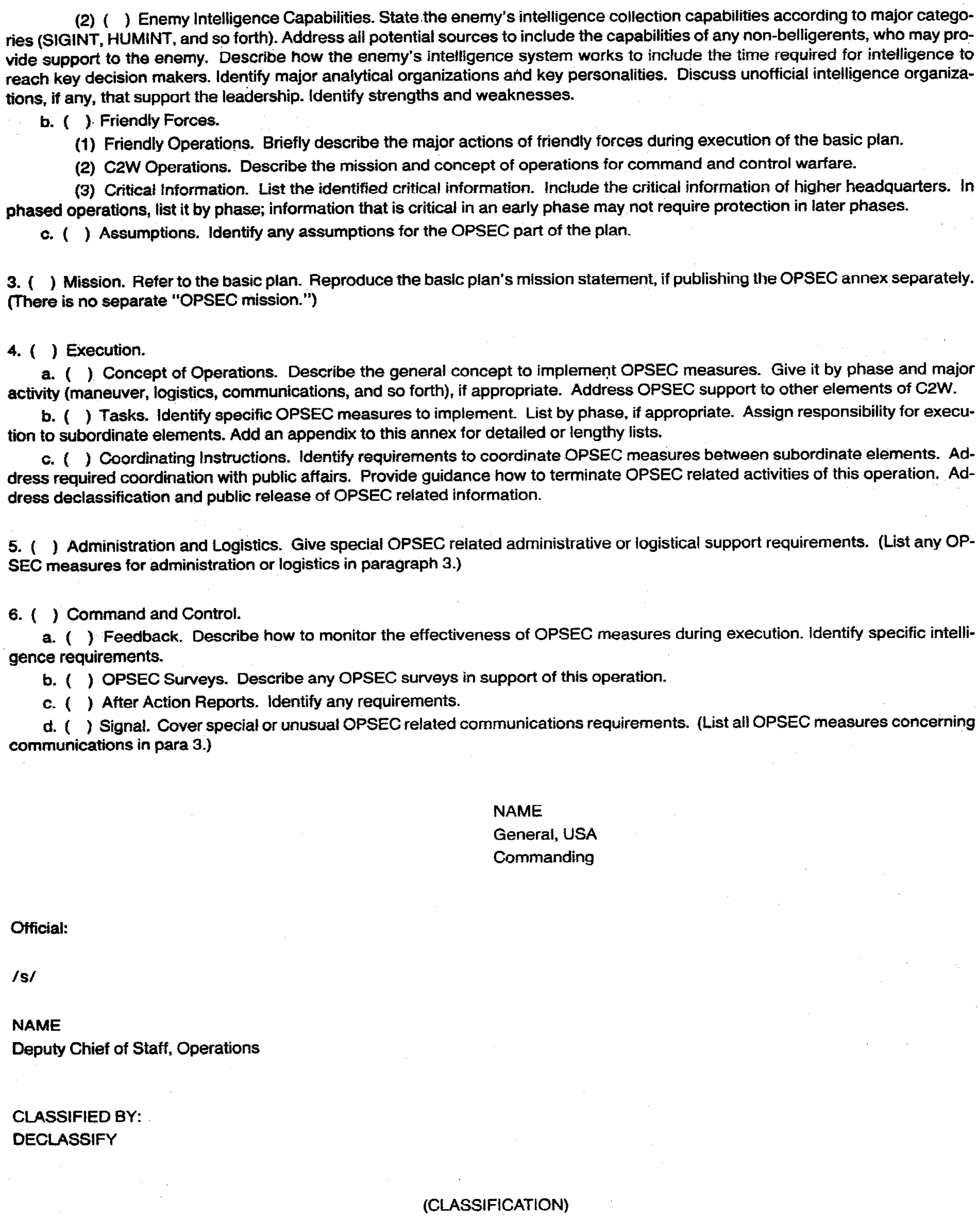
b. Reference documents needed to accomplish tasks stated herein.

2. ( ) Situation. Refer to other annexes and paragraphs in the basic plan as much as possible to avoid duplication. When publishing the OPSEC annex separately from the basic order, however, it is necessary to copy the information here in detail. That allows the OPSEC annex to be a useful, stand-alone document.

a. ( ) Enemy Forces.

(1) ( ) Current Enemy Intelligence Assessment. State the estimated enemy's assessment of friendly operations, capabilities, and intentions. Specifically address any known enemy knowledge of the friendly operation covered in the basic plan.

Figure L–1. Sample format OPSEC Annex - continued



(2) ( ) Enemy Intelligence Capabilities. State the enemy's intelligence collection capabilities according to major categories (SIGINT, HUMINT, and so forth). Address all potential sources to include the capabilities of any non-belligerents, who may provide support to the enemy. Describe how the enemy's intelligence system works to include the time required for intelligence to reach key decision makers. Identify major analytical organizations and key personalities. Discuss unofficial intelligence organizations, if any, that support the leadership. Identify strengths and weaknesses.

b. ( ) Friendly Forces.

(1) Friendly Operations. Briefly describe the major actions of friendly forces during execution of the basic plan.

(2) C2W Operations. Describe the mission and concept of operations for command and control warfare.

(3) Critical Information. List the identified critical information. Include the critical information of higher headquarters. In phased operations, list it by phase; information that is critical in an early phase may not require protection in later phases.

c. ( ) Assumptions. Identify any assumptions for the OPSEC part of the plan.

3. ( ) Mission. Refer to the basic plan. Reproduce the basic plan's mission statement, if publishing the OPSEC annex separately. (There is no separate "OPSEC mission.")

4. ( ) Execution.

a. ( ) Concept of Operations. Describe the general concept to implement OPSEC measures. Give it by phase and major activity (maneuver, logistics, communications, and so forth), if appropriate. Address OPSEC support to other elements of C2W.

b. ( ) Tasks. Identify specific OPSEC measures to implement. List by phase, if appropriate. Assign responsibility for execution to subordinate elements. Add an appendix to this annex for detailed or lengthy lists.

c. ( ) Coordinating Instructions. Identify requirements to coordinate OPSEC measures between subordinate elements. Address required coordination with public affairs. Provide guidance how to terminate OPSEC related activities of this operation. Address declassification and public release of OPSEC related information.

5. ( ) Administration and Logistics. Give special OPSEC related administrative or logistical support requirements. (List any OPSEC measures for administration or logistics in paragraph 3.)

6. ( ) Command and Control.

a. ( ) Feedback. Describe how to monitor the effectiveness of OPSEC measures during execution. Identify specific intelligence requirements.

b. ( ) OPSEC Surveys. Describe any OPSEC surveys in support of this operation.

c. ( ) After Action Reports. Identify any requirements.

d. ( ) Signal. Cover special or unusual OPSEC related communications requirements. (List all OPSEC measures concerning communications in para 3.)

NAME
General, USA
Commanding

Official:

/s/

NAME
Deputy Chief of Staff, Operations

CLASSIFIED BY:
DECLASSIFY

(CLASSIFICATION)

Figure L–1. Sample format OPSEC Annex

Glossary

Section I
Abbreviations

ACOUSINT
acoustical intelligence

AMC
Army Material Command

ARTEP
Army training and evaluation program

ASA(RDA)
Assistant Secretary of the Army (Research, Development and Acquisition)

AWRAC
Army Web Risk Assessment Cell

BOQ
bachelor officer quarters

CDRL
contract data requirements list

CI
counterintelligence

CJCS
Chairman, Joint Chiefs of Staff

COA
course of action

COE
Chief of Engineers

COMINT
communications intelligence

COMSEC
communications security

CPA
Chief of Public Affairs

C2
command and control

C2W
command and control warfare

C4
command, control, communications and computers

DA
Department of the Army

DCS, G-2
Deputy Chief of Staff for Intelligence

DCS, G-3/5/7
Deputy Chief of Staff for Operations and Plans —

DCS, G-1
Deputy Chief of Staff for Personnel

DEFCON
Defense condition

DOD
Department of Defense

DISC4
Director of Information Systems for Command, Control, Communications and Computers

EAC
echelons above corps

EEFI
essential elements of friendly information

EEI
essential elements of information

ELINT
electronic intelligence

ELSEC
electronic security

EMCON
emission control

EW
electronic warfare

FISINT
foreign instrumentation signals intelligence

FM
field manual

FIS
Foreign Intelligence Service

FOIA
Freedom of Information Act

HQDA
Headquarters, Department of the Army

HUMINT
human intelligence

IMINT
imagery intelligence

INSCOM
U.S. Army Intelligence and Security Command

ISS
information systems security

JCS
Joint Chiefs of Staff

LOC
lines of communication

MACOM
major Army command

MASINT
measurement and signature intelligence’

MD
military deception

MED
manipulative electronic deception

MOP
memorandum of policy

MTOE
modified table of organization and equipment

NCS
net control station

NOTAM
notice to airmen

ODCS, G-2
Office of the Deputy Chief of Staff for Intelligence

OIP
Organizational Inspection Program

OPLAN
operation plan

OPORD
operation order

OPSEC
operations security

PAO
public affairs office or officer

PEOs
Program Executive Officers

PM
Program manager/project manager/product manager

POC
point of contact

PSYOP —
psychological operations

RDT&E
research, development, test and evaluation

ROE
rules of engagement

SAP
special access program

SCA
Service Cryptologic Agency

SCG
security classification guide

SCI
sensitive compartmented information

SIGINT
signals intelligence

SIGSEC
signals security

SOI
signals operating instructions

SOP
standard operating procedure

SSG
staff sergeant

TDA
table of distribution and allowances

TDY
temporary duty

TRADOC
U.S. Army Training and Doctrine Command

UA
User Agency

USAF
U.S. Air Force

USAISC
U.S. Army Information Systems Command

USAITAC
U.S. Army Intelligence and Threat Analysis Center

USASSDC
U.S. Army Space and Strategic Defense Command

Section II
Terms

Adversary
Those individuals, groups or organizations that must be denied critical information to maintain friendly mission effectiveness.

Appreciations
Personal conclusions, official estimates and assumptions about another party's intentions, military capabilities and activities used in planning and decision-making.

a. Desired appreciations . Adversary personal conclusions and official estimates, valid or invalid, that result in adversary behaviors and official actions advantageous to friendly interests and objectives.

b. Harmful appreciations . Adversary personal conclusions, official estimates or assumptions, valid or invalid, that result in adversary behaviors and official actions harmful to friendly interests and objectives.

Battlefield deception
Those operations or measures conducted at echelons theater and below to purposely mislead enemy forces by distorting, concealing or falsifying indicators of friendly intent.

Command and control warfare
The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary command and control (C2) capabilities, while protecting friendly C2 capabilities against such actions.

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

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

Critical information
Specific facts about friendly intentions, capabilities and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequence for friendly mission accomplishment.

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

Essential elements of friendly information (EEFI)
Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities and activities, so they can obtain answers critical to their operational effectiveness.

Essential elements of information (EEl)
The critical items of information regarding the enemy and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision.

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

Field Test
Any test, demonstration, Advanced Concepts, Technologies Demonstrations reports, operational employment of equipment, personnel or exercise conducted at military installations, contractor facilities or on public or private domain, indoors or outdoors.

Force protection
Security program designed to protect soldiers, civilian employees, family members, facilities and equipment, in all locations and situations, accomplished through planned and integrated application of operations security, combating

terrorism, physical security, base defense, personal protective services, law enforcement and crime prevention, and supported by intelligence, counterintelligence and other security programs.

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

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 systems Security (ISS)
A composite of means to protect telecommunications systems, automated information systems and the information they process. The sub-disciplines of ISS include computer security, communications security, electronic security and control of compromising emanations.

Intelligence
The product resulting from collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries. 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.

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.

Multidiscipline counterintelligence analysis
The process of determining the presence and nature of the total all-source adversary intelligence threat to a given target in 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 compromise
The disclosure of sensitive or critical information which has been identified by the Command and all higher headquarters as jeopardizing the unit's ability to execute its mission or to adequately protect its personnel and/or equipment.

Operations security indicators
Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information

Operations security measures
Methods and means to gain and maintain essential secrecy about critical information. The following categories apply:

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

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

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

Publicly Accessible Web site
Army Web site with access unrestricted by password or PKI user authorization. "Public" refers to the at-large audience on the Internet; anyone who can access a Web site through a browser.

Operations security 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.

Operations security 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.

Psychological operations
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 psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP.

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 codeword 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
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. Examples which may be deemed sensitive include but are not limited to information related to: 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 compartmentation is essential. SCI rules are established by the Director of Central Intelligence and are covered in DOD 5105.21–M–1.

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. Overt contacts between people or 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.

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.

TEMPEST
An unclassified, short name referring to investigations and studies of compromising emanations. Sometimes used synonymously for the term "compromising emanations."

Threat
Capability of a potential enemy 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 on U.S. weapons Systems).

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

Transmission security
The component of communications security which results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

Section III
Special Abbreviations and Terms

There are no entries for this section.

Index

The organization of this index's alphabetical by topic and by subtopic within topic. Topics and subtopics list a paragraph number

USAPD

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER WIN32 Version 226

PIN:	003324–000
DATE:	10-13-05
TIME:	12:53:47
PAGES SET:	58

DATA FILE:	C:\WinComp\r530-1.fil
DOCUMENT:	AR 530–1
SECURITY:	UNCLASSIFIED
DOC STATUS:	REVISION