Army Regulation 530–1

Operations and Signal Security

Operations Security

Headquarters
Department of the Army
Washington, DC
26 September 2014

UNCLASSIFIED

SUMMARY of CHANGE

AR 530–1
Operations Security

This major revision, dated 26 September 2014--

- Updates operations security terms and definitions with Department of Defense and Joint usage (para 1-5).
- Adds Administrative Assistant to the Secretary of the Army responsibility for the HQDA operations security program (para 2-2).
- Adds guidance to authorize purchases of operations security awareness and training products (para 3-3).
- Adds Operations Security Level III training certification requirements (para 4-2c).
- Adds operations security and external official presence training requirements (para 4-3).
- Updates Joint and interagency training guidelines (para 4-4).
- Updates operations security assessment procedures (para 5-4).
- Updates operations security contractual documents review requirements (chap 6).
- Adds cyberspace critical information sample (app C-27).
- Updates guidance for Army Operations Security Annual Report Program (app I).
- Updates guidance for Annual Army Operations Security Achievement Awards Program (app J).
- Updates Army command, Army service component command, and direct reporting unit listing (app K).
- Updates Freedom of Information Act (Title 5, United States Code, Section 552) Exemption 2 guidance (app L).
- Adds operations security internal control evaluation (app O).
- Makes administrative changes (throughout).

Headquarters
Department of the Army
Washington, DC
26 September 2014

*Army Regulation 530–1

Effective 26 October 2014

Operations and Signal Security

Operations Security

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the Secretary of the Army

History. This publication is a major revision.

Summary. This regulation fully implements National Security Decision Directive 298, Chairman, Joint Chiefs of Staff Instruction 3213.01D, Joint Publication 3–13.3, and Department of Defense directive 5205.02E and Department of Defense 5205.02–M. This regulation states Army policy on operations security program development, revises terminology, provides details on the operations security planning process, and outlines the operations security review, assessment and survey requirements. The Army operations security program authority is consistent with Joint policy and doctrine in Chairman, Joint Chiefs of Staff Instruction 3213.01D and Joint Publication 3–13.3. In Joint and Army operations, operations security is an information-related capability integrated by Information Operations as prescribed in Joint Publication 3–13.

Applicability. This regulation applies to military and civilian personnel of the Active Army, the Army National Guard, the U.S. Army Reserve, and related activities of those organizations. Contractors must comply with contractually imposed operations security requirements. Also, if contractors have access to government information they are required to follow the same requirements for protection of sensitive, unclassified government information per Joint Ethics Regulation and Public Law. This regulation applies from conception of an activity or project and during all phases of operations, including training, readiness, and mobilization.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, G–3/5/7. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief with the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the 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 higher headquarters to the policy proponent. Refer to AR 25–30 for more information.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see app O).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from Deputy Chief of Staff, G–3/5/7 (G–39), 400 Army Pentagon, Washington, DC 20310.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the e-mail address at http://usarmy.pentagon.hqda.list.aoc-odci-2@mail.mil.

Distribution. This regulation 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 U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This regulation supersedes AR 530–1, dated 17 April 2007.

Contents—Continued

Contents—Continued

Appendixes

Figure List

Glossary

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

1–4. Responsibilities
Responsibilities are listed in chapter 2. Responsibilities referring to commanders and similar terms are equally applicable to equivalent management and supervision positions in organizations that do not employ a traditional military command structure.

1–5. Definitions
a. Operations security.

(1) As defined in Department of Defense Directive (DoDD) 5205.02E, OPSEC is a process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to—

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

(b) Determine indicators and vulnerabilities that adversary intelligence systems might obtain to be able to interpret or piece together to derive critical information in time to use against U.S. and/or friendly missions and poses an unacceptable risk.

(c) Select and execute measures that eliminate the risk to friendly actions and operations or reduce to an acceptable level.

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

(3) In concise terms, the OPSEC process identifies the critical information of military plans, operations, and supporting activities and the indicators that can reveal it, and then develops measures to eliminate, reduce, or conceal those indicators. It also determines when that information may cease to be critical in the lifespan of an organization's specific operation.

b. Critical information.

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

(2) Critical information consists of specific facts about friendly capabilities, activities, limitations (includes vulnerabilities), and intentions needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishment.

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

(4) Critical information can either be classified or unclassified depending upon the organization, activity, or mission. Critical information that is classified requires OPSEC measures for additional protection because it can be revealed by unclassified indicators. Critical information that is unclassified especially requires OPSEC measures because it is not protected by the requirements pertaining to classified information. Critical information can also be an action that provides an indicator of value to an adversary and places a friendly activity or operation at risk.

c. Sensitive information and controlled unclassified information (CUI). See DoD Manual 5200.01, Volume 4.

d. OPSEC compromise.

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

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

1–6. Requirement

a. The National OPSEC Program outlined in National Security Decision Directive 298 (NSDD 298) requires each executive department and agency with a national security mission to have an OPSEC program. Likewise, DoDD 5205. 02E supports the national program and requires each DoD component to have an OPSEC program.

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

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

(2) Traditional security programs to deny adversaries classified, sensitive, and/or critical information include—

(a) Information security.

(b) Information assurance.

(c) Electronic security.

(d) Emission security.

(e) Military deception.

(f) Physical security.

(g) Program protection planning.

(h) Personnel security.

(i) Industrial security.

c. OPSEC provides a methodology to manage risk. It is impossible to avoid all risk and protect everything. To attempt complete protection diverts resources from actions needed for mission success.

1–7. Application

a. OPSEC awareness and execution is crucial to Army success. OPSEC is applicable to all personnel, missions, and supporting activities on a daily basis. OPSEC denies adversaries information about friendly capabilities, activities, limitations, and intentions that adversaries need to make competent operational decisions. Without prior knowledge of friendly actions, adversary leaders cannot act effectively to prevent friendly mission accomplishment. It applies to all Army activities and is required during training, sustaining, mobilizing, preparing for, and conducting operations, exercises, tests, or activities.

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

(2) Combat capability increasingly depends upon gaining and maintaining information superiority. This impacts all aspects of raising, equipping, training, deploying, employing, and sustaining forces. Every Army organization produces or has information that ultimately affects the ability of U.S. forces to accomplish missions. Every organization must identify and protect this information (for example, emerging tactics, techniques and procedures) which an adversary could use against U.S. forces.

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

(4) Army program executive officers (PEOs), program, project, or product managers, and contracting officials must consider OPSEC as a stipulation in all contracts. All requirements packages must receive two OPSEC reviews by the requiring activity (RA) OPSEC officer.

(a) At the beginning of the contracting process to determine if OPSEC requirements are needed in the performance work statement (PWS).

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

(5) 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. Prior coordination with the foreign disclosure officer must be conducted before sharing government information with any foreign official.

(a) Intermediate-range nuclear forces, the Chemical Weapons Convention and the new Strategic Arms Reduction Treaty agreements have provisions for on-site inspections. Under the Chemical Weapons Convention, challenge inspections may occur at sites and in buildings that have nothing to do with declared chemical weapons activity. Regional multi-national treaties, such as the Conventional Armed Forces in Europe Treaty or the Vienna Document

2011, affect Army units stationed on host country territory. Army units can be subject to observations of unit activity in garrison or while deployed on the territory of a country which is also a treaty participant. With only 72 hours of advance notice, the Open Skies Treaty allows reconnaissance over flights anytime, anywhere, with few exceptions.

(b) These agreements, while enhancing U.S. national security, provide adversaries with opportunities to collect sensitive and/or critical information unrelated to the treaties. Each Army organization or activity must have an OPSEC plan/standing operating procedure (SOP) to protect sensitive and/or critical information unrelated to legitimate inspection aims. The plan/SOP must direct immediate implementation of OPSEC measures for daily vulnerabilities. This may help to avoid compromise of sensitive and/or critical information and activities that are likely collateral collection targets of these foreign inspections unrelated to the treaties. The plan/SOP must also have additional measures that are specific for a particular inspection regime. These additional OPSEC measures must be ready for implementation immediately after notice of an impending inspection.

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

1–8. Proponent

The Deputy Chief of Staff (DCS), G–3/5/7 is the Army's proponent for OPSEC. At lower echelons, the command, unit, activity, or installation operations officer is the staff proponent for OPSEC. OPSEC is an operations function that denies critical information and requires close integration with other security programs. While OPSEC is not an intelligence function, it relies heavily upon intelligence processes in threat determination and program effectiveness evaluation.

Chapter 2
Responsibilities

2–1. Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

In addition to the requirements outlined in paragraphs 2–18, 2–19 and 2–22, the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) will—

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

b. Ensure all individuals who perform acquisition duties receive OPSEC training (see chap 4 of this regulation) in support of program protection planning.

2–2. Administrative Assistant to the Secretary of the Army

In addition to the requirements outlined in paragraphs 2–8, 2–18, 2–19 and 2–22, the Administrative Assistant to the Secretary of the Army will—

a. Appoint a HQDA Staff OPSEC PM with the responsibility for the OPSEC program for HQDA Staff and Secretariat.

b. The HQDA Staff OPSEC PM will have the following responsibilities:

(1) OPSEC tasking authority.

(2) Provide guidance for OPSEC reviews for official information released to the public.

(3) Conduct assessments for HQDA principal organizations.

(4) The HQDA Staff OPSEC PM will be a separate position from the Army OPSEC PM in DCS, G–3/5/7 (G–39).

2–3. Chief Information Officer/G–6

In addition to the requirements outlined in paragraph 2–18, 2–19 and 2–22, the Army Chief Information Officer/G–6 will—

a. Ensure the development and integration of Army command, control, communications, and computer systems include OPSEC to protect sensitive and/or critical information.

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

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

d. Prescribe guidance pertaining to evolving voice, data, wireless, and other technologies as they apply to Army OPSEC programs per AR 380–53 and National Telecommunications and Information Systems Security Directive (NTISSD) No. 600.

2–4. The Inspector General

In addition to the requirements outlined in paragraph 2–18, 2–19 and 2–22, the Inspector General will—

a. Ensure OPSEC is an item of interest in all inspections of organizations throughout the Army.

b. Coordinate annually with the Army OPSEC PM on applicable OPSEC-related matters to ensure consistency with this AR.

2–5. Office of the Chief of Public Affairs (OCPA)

In addition to the requirements outlined in paragraph 2–18, 2–19 and 2–22, OCPA will—

a. Provide guidance on the public release of all official information to ensure the protection of sensitive and/or critical information.

b. Requires OPSEC be considered before any public release of DoD information, to include information to be published or released by DoD-affiliated persons in their private capacity. See AR 360–1 for additional information.

c. Provide assistance to the Army OPSEC PM in increasing OPSEC awareness throughout the Army.

2–6. Deputy Chief of Staff, G–2

In addition to the requirements outlined in paragraph 2–18, 2–19 and 2–22, the DCS, G–2 will—

a. Assist other Army staff organizations, agencies, and TRADOC in the development of training and doctrine programs pertinent to all intelligence and CI aspects of OPSEC.

b. Render foreign disclosure decisions regarding controlled unclassified information in accordance with AR 380–10.

c. Serve as the proponent for program management of intelligence and CI support to OPSEC programs.

d. Incorporate OPSEC policy into AR 380–49.

e. Support integration of OPSEC as a measure in PPPs through the Army Research and Technology Protection Center.

2–7. Deputy Chief of Staff, G–3/5/7

In addition to the requirements outlined in paragraph 2–18, 2–19 and 2–22, the DCS, G–3/5/7 will designate a full-time Army OPSEC PM with the grade of O–5 or above, or DA civilian equivalent. The Army OPSEC PM will—

a. Develop Army OPSEC objectives, policies, and procedures in AR 530–1 consistent with applicable DoDDs and Joint publications.

b. Provide guidance and oversight to ACOM, ASCC, and DRU OPSEC PMs ensuring OPSEC compliance is maintained in accordance with established and regulatory guidance.

c. Review and evaluate, annually, the Army's OPSEC posture and the effectiveness of ACOM, ASCC, and DRU OPSEC programs; provide guidance and assistance as required.

d. Identify resource requirements for the Army OPSEC Program.

e. Coordinate, supervise, and execute DA OPSEC working groups with ACOM, ASCC, and DRU OPSEC PMs, and the OSE.

f. Coordinate with the Army OSE for training, policy development, and execution of the Army OPSEC Program.

g. Coordinate for funding of elements providing OPSEC training support to the Army OPSEC Program.

h. Facilitate coordination with TRADOC and OSE for the development of OPSEC doctrine and the integration of OPSEC instruction at Army schools and training centers.

i. Coordinate the Army program and maintain routine contact with the Joint Staff, other Services, and DOD.

j. Submit the Army's Annual OPSEC Report to the Office of the Under Secretary of Defense, Intelligence (OUSD(I)), as directed.

k. Represent DA on interagency committees.

l. Integrate intelligence and counterintelligence support into OPSEC planning and implementation, with the assistance of DCS, G–2 and other intelligence agencies.

2–8. Commanders of Army commands, Army service component commands, and direct reporting units

Note. See appendix K of this regulation or AR 10–87 for a complete listing of Army commands (ACOMs), Army service component commands (ASCCs), and direct reporting units (DRUs). Also, this regulation applies to executive directors as well as military commanders. For HQDA, the Administrative Assistant to the Secretary of the Army exercises the same authorities as commanders of ACOMs and ASCCs, as prescribed by regulation, policy, delegation, or other issuance. In addition to the requirements outlined in paragraphs 2–18, 2–19 and 2–22, commanders will—

a. Appoint a command OPSEC PM in writing.

(1) Because of the significance of OPSEC at this level of command and authority, the commander will ensure the command's OPSEC PM is a full-time duty position. The command OPSEC PM is responsible for numerous OPSEC programs within the command and provides guidance and oversight and coordinates their actions under the command's OPSEC program. Dependent on the workload, an OPSEC officer or coordinator may be necessary to assist the

command's OPSEC PM. Requests for waivers, with established justification, shall be signed by the commander and submitted to the Army OPSEC PM at DCS, G–3/5/7 (G–39).

(2) The individual will be an experienced commissioned officer (at least an O–4 or W–3) or civilian equivalent. The commander can approve an exception to these rank/grade levels, in writing.

(3) Because contractors do not have authority over U.S. military and government personnel and cannot represent the position of the U.S. Government, contract employees will not be assigned as the command's OPSEC PM or OPSEC officer. However, they may perform OPSEC duties in a supporting capacity as an OPSEC coordinator so long as they do so under the supervision of a U.S. government employee or servicemember.

b. Develop and implement functioning, active, and documented (formal) OPSEC programs for staff organizations within the command to meet their specific needs and to support the command's OPSEC program.

(1) With the assistance of the command's OPSEC PM, commanders will decide which staff organizations within their command will develop and implement a formal OPSEC program.

(2) The guiding principle to determine whether a staff organization will have a formal OPSEC program is based on the sensitivity, visibility, and uniqueness of its mission.

(3) Commanders may decide to incorporate a subordinate staff organization under a higher echelon staff organization's OPSEC program. Commanders shall mandate that a subordinate staff organization determine their critical information and develop OPSEC measures to protect their critical information.

(4) Regardless of the level of implementation of OPSEC programs, every staff organization must have its own OPSEC program or be covered under a higher echelon staff organization's OPSEC program.

c. Ensure ACOM, ASCC, and DRU OPSEC PMs maintain routine contact with the Army OPSEC PM. ACOM, ASCC, and DRU OPSEC PMs will provide updates, status reports, OPSEC issues, OPSEC compromises, lessons learned, initiatives, requests for support, recommendations, personnel turnover, verification of contact information, media contacts, and so forth.

d. Submit the command's annual OPSEC report for the fiscal year to the Army OPSEC PM. Sample guidance and a list of representative data elements are provided in appendix I of this regulation.

e. Ensure command OPSEC programs are examined as part of the Organizational Inspection Program outlined in AR 1–201.

f. Ensure OPSEC annual training guidance is provided to subordinate elements.

g. Identify OPSEC resource requirements through their command's program objective memorandum process.

h. Identify and resource additional OPSEC personnel requirements as required.

i. Participate in HQDA-level OPSEC working groups and conferences.

2–9. Commander, Training and Doctrine Command (TRADOC)

In addition to the requirements outlined in paragraphs 2–8, 2–18, 2–19 and 2–22, the Commander, TRADOC will—

a. Develop OPSEC doctrine for the Army, if necessary.

b. Ensure OPSEC instruction is included in all TRADOC schools.

c. Ensure appropriate levels of updated OPSEC instruction are incorporated into the programs of instruction (POIs) for all Army accession and professional development courses.

d. Integrate OPSEC into doctrine and Army education and training as appropriate. This includes, but is not limited to, courses, training support packages, Soldier training publications, and combined arms training strategies.

e. Ensure OPSEC measures are incorporated into Army combat development activities to include concepts for doctrine, organizations, and materiel.

f. Ensure TRADOC capability managers provide acquisition managers with operational considerations so that OPSEC is addressed throughout the lifecycle of any acquisition program.

2–10. Commander, U.S. Army Materiel Command (AMC)

In addition to the requirements outlined in paragraphs 2–8, 2–18, 2–19 and 2–22, the Commander, AMC will—

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

b. Ensure a consistent and effective level of OPSEC protection is applied to all systems in life cycle testing and development, in coordination with DCS, G–3/5/7 (G–39), the U.S. Army Information Systems Engineering Command, and Assistant Secretary of the Army (Acquisition, Logistics, and Technology).

c. Provide research and development regarding camouflage and deception for fixed installations, ranges, and test facilities under the cognizance of AMC, in coordination with the Chief of Engineers.

2–11. Commander, U.S. Army Intelligence and Security Command (INSCOM)

In addition to the requirements outlined in paragraphs 2–8, 2–18, 2–19 and 2–22, the Commander, Intelligence and Security Command will—

a. Provide data on the foreign intelligence threat, terrorist threat, and CI support to OPSEC programs for ACOMs,

ASCCs, DRUs, and above. INSCOM will provide information updates, but will not write threat assessments for the supported command or agency. (The supported organization's intelligence staff element performs this function.)

b. Advise and assist supported commands in electronic warfare matters and provide technical support to manipulative electronic deception activities that relate to OPSEC, as resources permit.

2–12. Commander, U.S. Army Criminal Investigation Command

In addition to the requirements outlined in paragraphs 2–8, 2–18, 2–19 and 2–22, the Commander, U.S. Army Criminal Investigation Command will provide criminal threat intelligence as requested to support Army OPSEC programs. Provide appropriate investigative support as requested by organization commanders or agency directors in resolving reported OPSEC compromises depending on nature and circumstances of compromise.

2–13. Commanding General, Installation Management Command

In addition to the requirements outlined in 2–8, 2–18, 2–19 and 2–22, the Commander, IMCOM will—

a. Provide OPSEC oversight of garrison commanders.

b. Provide OPSEC guidance to installation OPSEC working groups such as, but not limited to, CIL development and dissemination, and updated areas of emphasis.

c. Coordinate with U.S. Army Corps of Engineers to develop and publish material and design criteria and techniques required to incorporate counter surveillance measures in fixed installations and facilities constructed for the Army.

d. Develop and provide guidance to all Army organizations working with Base Realignment and Closures (BRAC) to identify and ensure protection of BRAC-related critical information.

2–14. Commander, Army Test and Evaluation Command and commanders, subordinate commanders, and directors of major test ranges, centers, and facilities

In addition to the requirements outlined in paragraphs 2–8, 2–18, 2–19 and 2–22, the Commander, ATEC will—

a. Develop and implement a formal OPSEC program, as described in paragraph 2–3a, above, for range or test facilities and OPSEC plans/guidance for all tests, experiments, and evaluations.

b. Implement system OPSEC guidance from PEOs and PMs to ensure the protection of sensitive and critical information. Test activities will augment the PEO/PM guidance with guidance based on local OPSEC considerations and threats.

c. Disseminate the OPSEC plan and critical information for each program, project, or activity using the range or test facilities involved in ATEC-conducted tests, experiments, and evaluations to all participating organizations and individuals, to include support staff.

d. Coordinate OPSEC measures between all range and test facility users and participants in ATEC tests, experiments, and evaluations. Assist users to implement OPSEC measures.

e. Request range users provide their CPI and CIL. This will allow the range OPSEC officer to conduct coordination as required to ensure any required OPSEC support is provided. This includes range user guidance concerning approval of public release of information about the range user.

f. In order to release information not owned by ATEC into the public domain, the information must be approved, reviewed and receive concurrence, in writing or via email, by the PEOs, PMs or owners of that information.

g. If information is not owned by ATEC ensure the PM removes markings or changes to the information including distribution statements.

2–15. Commander, 1st Information Operations Command (Land)

In addition to the requirements outlined in paragraphs 2–18, 2–19 and 2–22, the 1st IO CMD will provide direct support and resources to the DCS, G–3/5/7 (G–39), as the responsible agency in support of Army-wide OPSEC through the Army operation security support element (OSE).

2–16. Army operations security support element

The Army OSE will—

a. Conduct OPSEC assessments and provide planning support to ACOMs, ASCCs, DRUs, and operational units, installations, and activities.

b. Provide OPSEC training and mobile training teams through the direction of the Army OPSEC PM and as requested by ACOMs, ASCCs, DRUs, and operational units, installations, and activities.

c. Support TRADOC as the IO proponent in the development of OPSEC doctrine, training, and tactics, techniques, and procedures.

d. Support DCS, G–3/5/7 (G–39) in the development of OPSEC policy.

e. Support DCS, G–3/5/7 (G–39) with the coordination of OPSEC matters affecting intra-service, Joint, and DoD components. Represent Army at Joint, DoD, and national OPSEC conferences, working groups, and symposiums, when needed.

f. Support DCS, G–34, Army Protection Program Assessments.

g. Provide HQDA-accredited OPSEC officer training as needed, in coordination with the Army OPSEC PM. The OSE will also advise units requesting alternatives for Army OPSEC training.

h. Manage Level II OPSEC training for OPSEC officers and Level III OPSEC certification for HQDA OPSEC Officer or interagency operational security support staff (IOSS) course instructors by maintaining records of completion as well as conducting quality control of the training to ensure standardization of OPSEC training throughout the Army. Also, award Project Development Skill Identifier H1B (OPSEC Practitioner Specialist) to all course eligible military personnel upon completion of the HQDA OPSEC or IOSS courses.

i. Develop, maintain, and update the Army's OSE Web site(s) currently at https://www.us.army.mil/suite/page/589183/.

j. Monitor, evaluate, and provide advice to the Army OPSEC PM regarding OPSEC activities.

k. Provide OPSEC red teaming support (per DOD IO Roadmap).

l. Provide appropriate investigative support as requested by DCS, G–3/5/7 (G–39), in resolving reported OPSEC compromises.

m. Develop OPSEC POIs, as needed.

n. Coordinate the Army OPSEC program along with the Army OPSEC PM, and maintain routine contact with the Joint Staff, other Services, and DOD.

o. Ensure coordination with the Army Web risk assessment cell (AWRAC) in tracking and maintaining the status of potential OPSEC compromises in all open source media and their impact on the IO environment is established. Incorporate OPSEC compromise statistics in annual trends and analysis reporting. The OSE will provide final reviews, analyses, and assessments of OPSEC compromises to the Army OPSEC PM. For more AWRAC information, see paragraph 2–20 of this regulation.

p. Analyze and recommend mitigation measures for reported OPSEC compromises.

2–17. Army Web risk assessment cell

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

a. Conduct random sampling of Army Web sites or review requested Web sites to identify security concerns.

b. Notify Web site owners or IA PMs of suspected concerns and suspense dates for reporting corrective action. Provide guidance to Web site owners and IA PMs to ensure Army Web sites are compliant with other DOD and Army Web site IA policies.

c. Conduct random reviews of Web sites for disclosure of critical and/or sensitive information. Web sites include, but are not limited to, FRG pages, unofficial Army Web sites, external official presence (EOP) Web sites, Soldiers' blogs, and personal published or unpublished works related to the Army. The AWRAC will ensure a review and analysis is conducted on the suspected data found on the Internet.

d. As required, report deficiencies and corrections to the Army OSE, DCS, G–3/5/7 (G–39), the Army Cyberspace Operations Integration Center, and the requesting/affected command.

e. Identify trends and provide statistical data to the Army OSE.

2–18. Commanders and directors of units, activities, and installations at battalion and higher echelons

Note. For the purpose of this regulation, a unit or activity is at battalion-level or a higher echelon when its commander or director is a lieutenant colonel (or civilian equivalent) or higher. This applies to any unit or activity authorized by either a modified table of organization and equipment or a table of distribution and allowances. This section applies to all four categories of command- operations, strategic support, recruiting and training, and installation. Garrison commands have additional requirements in paragraph 2–22 of this regulation. Program executive officers, program, project, and product managers are addressed in paragraph 2–21 of this regulation. The Headquarters, Department of the Army (HQDA) Staff, Army command, Army service component command, and direct reporting unit staff organizations are addressed in paragraph 2–8.

a. In addition to the requirements outlined in paragraph 2–8, 2–18, 2–19 and 2–22, commanders at battalion and higher echelons will develop and implement a functioning, active, and documented (formal) OPSEC program for their unit, activity, or installation to meet their specific needs and to support the OPSEC programs of higher echelons. To develop and implement a formal OPSEC program, commanders will—

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

(2) Appoint an OPSEC PM/officer/coordinator, in writing, with responsibility for supervising the execution of proper OPSEC within their organization.

(3) Ensure the appointed OPSEC PM/officer/coordinator and alternate receive appropriate training per chapter 4 of this regulation, and they are of sufficient rank or grade to execute their responsibilities.

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

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

(6) Approve the unit, activity, or installation critical information list (CIL). (The OPSEC PM/officer/coordinator will develop and propose the CIL to the commander for approval.)

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

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

(7) Approve OPSEC measures and length of time for implementation.

(8) Conduct a risk assessment to determine what OPSEC measures are necessary and their impact to the mission and then decide what OPSEC measures to implement.

(9) Publish OPSEC measures that must be practiced on a consistent basis in OPSEC document(s). Publish OPSEC measures specific to an operation, exercise, or activity in operation plans (OPLANs) and operation orders (OPORDs) or in OPSEC-directive type document(s).

(10) Ensure the OPSEC program addresses all personnel with access to sensitive and/or critical information (for example, Soldiers, civilians supporting the military, contractors, Family members, local national employees, and all other individuals who have access).

(11) Ensure OPSEC is incorporated and emphasized to Family Readiness Support Assistants (FRSAs) and FRGs. This emphasis shall not be limited to periods of deployment or mobilization.

(12) Ensure OPSEC is incorporated into all contractual requirements and contracts, both classified and unclassified, involving sensitive and/or critical information (see chap 6–2 of this regulation).

(13) Provide appointed OPSEC program manager/officer/coordinator with opportunities for attendance at other OPSEC-related courses, conferences, and meetings.

(14) Ensure the public affairs review process includes an OPSEC review to prevent the release of sensitive and/or critical information which includes U.S. information that is determined to be exempt from public disclosure according to DoDD 5230.09, DoDD 5230.25 and DoDD 5400.07 or that is subjected to export controls according to ITAR, EAR, 15 CFR 768.1 et seq., AR 360–1, AR 70–14, AR 25–30, and AR 380–5, and this regulation. A public affairs-qualified NCO/DA civilian/officer may conduct this review. If unsure the information is releasable, the public affairs officer (PAO) should consult the OPSEC officer of the owner of the information.

(15) Commanders will ensure all OPSEC PMs/officers/coordinators, information operations (IO) professionals, PAOs, FOIA officers, speechwriters, contracting specialists, FDOs, and personnel responsible for the review and approval of information intended for public release receive OPSEC training tailored to their duties. The popularity and availability of a variety of Internet-based services (social networking sites, photo sharing, Web log (blogs), and so forth) have greatly increased the risk of inadvertent disclosures of sensitive and/or critical information and possibly classified information (alone or through compilation). The fact these capabilities can be accessed from an ever increasing number of mobile devices in addition to the traditional desktop workstation reduces the amount of reaction time available and also increases the risk to sensitive and/or critical information. This threat can be mitigated through OPSEC awareness training and guidance for those using these Internet-based capabilities.

(a) The designated reviewer(s) will conduct routine reviews of unit/organization Web sites on a quarterly basis to ensure each Web site is in compliance with the policies of AR 25–1, and the content remains relevant and appropriate and void of critical and/or sensitive information indentified on the CIL. All OPSEC reviews will be documented.

(b) The minimum review will include all of the Web site management control checklist items in AR 25–1. Information contained on publicly accessible Web sites is subject to the policies and clearance procedures prescribed in AR 360–1 for the release of information to the public.

(c) Commanders will ensure their organizations will not make critical and sensitive information available on publicly-accessible Web sites.

b. Commanders may mandate that subordinate commands below battalion-level develop and implement a formal OPSEC program as described in paragraph 2–18*a* of this regulation, especially if these units have unique, highly visible, or highly sensitive missions.

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

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

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

d. Submit annual OPSEC report to higher headquarters.

2–19. Commanders at all levels, agency directors

Note. For the purpose of this regulation, this designation applies to all four categories of command operations-strategic support, recruiting and training, and installation. In addition, this regulation applies to executive directors, as well as military commanders.

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

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

c. Commanders will ensure their OPSEC program or OPSEC measures are coordinated and synchronized with supported organizations and supporting higher command's OPSEC program and security programs, such as information security (INFOSEC), IA, physical security, and force protection.

d. Commanders will ensure all official information released to the public domain receives an OPSEC review by a level II trained OPSEC PM, OPSEC officer, or OPSEC coordinator prior to dissemination. For public affairs personnel, please see AR 360–1 and paragraph 2–18a(14) of this document for more details.

e. Commanders will ensure all OPSEC program documents are reviewed at least annually to ensure changes in mission, threat, critical information lists (CILs), or OPSEC measures are reflected in plans/SOPs in a timely manner. Annual reviews should also assess if adequate resources are on hand to establish and maintain a successful program. In addition, annual reviews should reflect whether OPSEC support elements are being utilized and how effective OPSEC documents are, and if education, training, and awareness is being conducted throughout the workforce. A memorandum attached to an OPSEC document that is more than a year old can be used to verify the document has been reviewed and there are not any changes.

f. Commanders will ensure critical infrastructure program (CIP) efforts are supported in accordance with AR 525–26 when necessary.

g. Tenant units will coordinate with the garrison OPSEC officer and participate in the garrison installation-level OPSEC working groups as required.

2–20. Garrison commanders

In addition to the requirements outlined in paragraphs 2–18, 2–19 and 2–22, garrison commanders will—

a. Direct the establishment of a garrison-level OPSEC working group to advise and support installation operations, threats, and force protection working groups.

b. Coordinate OPSEC actions among the tenant organizations and facilitate OPSEC guidance to them. A garrison-level OPSEC working group can include, but is not limited to, tenant organization OPSEC officers, PAOs, security managers, antiterrorism officers, force protection officers, provost marshal office, network enterprise center, and so forth.

c. Consolidate and coordinate CIL from all tenant organizations to assist with the protection of other tenant organizations' critical and sensitive information.

d. Incorporate OPSEC into installation training and exercises, and encourage tenant organizations to practice OPSEC measures in a garrison environment.

e. Incorporate, as appropriate, countersurveillance measures in the construction of fixed installations and facilities for the Army.

f. Comply with installation commander guidance in case of Joint basing. The installation commander will direct the establishment of OPSEC working groups to advise and support installation operations and force protection working groups. For example, on Andrews Air Force Base, the Air Force is the installation commander, so the Air Force would be responsible for establishing an OPSEC working group.

2–21. Program executive officers and program, project, or product managers

a. Program executive officers and PMs will protect critical program information (CPI) by developing and implementing a formal OPSEC program as described in paragraph 2–18*a*, of this regulation. According to DoDI 5200.39, CPI is defined as elements or components of a research, development, and acquisition program that, if compromised, could cause significant degradation in mission effectiveness, shorten the expected combat-effective life of the system, reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. This includes classified military information or CUI about such programs, technologies, or systems. CPI is a form of critical information specific to acquisition programs.

b. PEOs and PMs will identify CPI as early as possible in the research, technology development, and acquisition

process, but not later than when a DoD agency or military component demonstrates an application for the technology in an operational setting, in support of a transition agreement with a pre-systems acquisition or acquisition program, or in exceptional cases, at the discretion of the laboratory/technical director. PEOs and PMs with identified CPI will submit program protection plans (PPPs) for review by the Army Systems Acquisition Review Council and Defense Acquisition Board, as required. Each PPP will include the employment of OPSEC measures for the protection of CPI, as defined in DoDI 5200.39 and DoDM 5200.01 (for each site where CPI has been identified or located). DoDI 5200. 39, under the authority of DoDI 5000.02, requires the integration of all countermeasures, to include OPSEC, that are adopted for the protection of CPI.

c. For programs not subject to the Defense Acquisition Board or Army Systems Acquisition Review Council review, PEOs and PMs will address the PPP requirement as part of the Milestones B and C review package. The respective milestone decision authority will be the approval authority.

d. 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 the contracting officer's technical representative or contracting officer's representative have the OPSEC plans reviewed 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.

e. Contracts that involve sensitive and/or critical sensitive information must have a contractor-developed or a RA-written OPSEC plan or annex to a security plan and must be approved by the RA OPSEC officer.

2–22. All Army personnel

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

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

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

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

b. In organizations without a specified operations staff, the element with primary responsibility for planning, coordinating, and executing the organization's mission activities will be the proponent for OPSEC.

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

d. Know what their organization considers to be sensitive and/or critical information, where it is located, who is responsible for it, how to protect it, why it needs to be protected, and who the unit OPSEC officer is.

e. Protect from unauthorized disclosure any sensitive and/or critical information to which they have personal access, to include sensitive and/or critical information from other branches of Service or foreign governments, and contractor proprietary information.

(1) Commanders will issue orders, directives, and policies for unit or organization personnel to protect sensitive and/or critical information in order to clearly define the specific OPSEC measures all personnel will practice. Prompt and appropriate action must be taken concerning a violation of the provisions of this regulation, especially in those cases involving incidents which can put missions and forces at unacceptable risk. Such actions will focus on a correction or elimination of the conditions that caused or contributed to the incident.

(2) A failure to comply with these orders, directives, or policies may be punished as violations of a lawful punitive order under Article 92 of the Uniform Code of Military Justice (UCMJ) or under other disciplinary, administrative, or other actions as applicable. Local OPSEC orders, directives and policies should expressly note that they are punitive.

(3) Personnel not subject to the UCMJ who knowingly, willfully, or negligently fail to protect sensitive and/or critical information from unauthorized disclosure may be subject to administrative, disciplinary, contractual, or criminal action. This should be expressly noted in local OPSEC orders, directives and policies.

f. Prevent unauthorized disclosure of sensitive and/or critical information.

(1) Do not publicly disseminate or publish photographs displaying sensitive and/or critical information.

(2) Do not publicly reference, disseminate, confirm, publish, or further propagate sensitive and/or critical information that has already been compromised, as this provides further unnecessary exposure of the compromised information and may serve to validate it. See AR 380–5 for further guidance.

g. Implement OPSEC measures as ordered by the commander, director, or an individual in an equivalent position.

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

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

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

(1) This includes all voice, text, technical data communications, and other emerging Internet-based capabilities (IbC).

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

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

l. Destroy (burn, shred, and so forth) sensitive and/or critical information that is no longer needed to prevent the inadvertent disclosure and reconstruction of this material per applicable standards. See AR 380–5 for further guidance.

Chapter 3
Policy and Procedures

3–1. General

OPSEC applies throughout the range of operations across the spectrum of conflict to all Army operations and supporting activities. All Army units, activities, agencies, installations, and staff organizations at battalion-level and higher, including equivalent table of distribution and allowances organizations will have functional, active, and documented OPSEC programs. These programs will use the process described in this chapter to identify and protect critical information.

3–2. Operations security programs

A functional, active, and documented OPSEC program will have the following common features: an OPSEC PM or OPSEC officer; the use of the five-step OPSEC process; an OPSEC document(s) to document the unit, activity, installation, or staff organization's critical information and OPSEC measures to protect it; and the coordination of OPSEC with other security programs.

a. An OPSEC program has an OPSEC PM or OPSEC officer appointed in writing or on orders by the commander or designated approval authority.

(1) An OPSEC PM is responsible for the development, organization, and administration of an OPSEC program at an ACOM, ASCC, DRU, installation, garrison, and corps. The OPSEC PM provides guidance and oversight to multiple subordinate OPSEC programs of various units, activities, and organizations, and coordinates their actions under the command's OPSEC program. OPSEC PMs are also OPSEC officers, but because of the extent and complexity of the OPSEC program they oversee, they are primarily referred to as OPSEC PMs.

(2) An OPSEC officer is responsible for identifying and protecting critical information related to Defense Critical infrastructure (DCI) with appropriate OPSEC measures and advising supporting contractors of information protection requirement. In fulfilling this responsibility, OPSEC PMs shall:

(a) Work with Defense Critical Infrastructure Program (DCIP) planners to identify and protect, through the use of OPSEC measures, critical information related to DCIP plans and programs and to integrate DCIP into OPSEC assessments and surveys as needed.

(b) Assist DCIP planners in promoting information sharing while safeguarding information that could harm DoD operations or that could jeopardize information-sharing agreements among stakeholders.

(3) An OPSEC officers is responsible for the development, organization, and administration of an OPSEC program at division-level and below.

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

(a) The appropriate rank/grade level for OPSEC program managers and OPSEC officers is as follows:

1. ACOM, ASCC, DRU, installation, corps. An experienced commissioned officer (at least O–4 or W–3), or DA civilian equivalent.

2. Division. O–3 or above, W–2 or above, NCO (E–8 or above), or DA civilian equivalent.

3. Brigade. O–3 or above, warrant officer, NCO (E–7 or above), or DA civilian equivalent.

4. Battalion. O–2 or above, warrant officer, NCO (E–6 or above) or DA civilian equivalent.

5. Below battalion-level. Any officer, warrant officer, NCO (E–5 or above) or DA civilian equivalent, as required.

(b) The commander can approve, in writing (in the appointment memorandum/order), an exception to the rank/grade levels listed above.

(c) Activities, installations, and other organizations that do not employ a traditional military command structure will determine the appropriate rank/grade level for their OPSEC PMs and OPSEC officers.

(d) Because contractors do not have authority over U.S. military and government personnel, contract employees will not be assigned as the command's primary OPSEC PM or OPSEC officer. However, they may perform OPSEC duties in a supporting capacity under the supervision of a service member or DA civilian employee.

(5) OPSEC PMs and OPSEC officers will receive appropriate training for their duty positions (see chap 4 of this regulation).

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

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

(a) Identification of critical information. Determine what information needs protection.

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

(c) Analysis of vulnerabilities. Analyze what critical information friendly forces are exposing.

(d) Assessment of risk. Assess what protective measures should be implemented.

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

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

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

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

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

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

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

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

d. The OPSEC program must be coordinated and synchronized with other security programs, such as the command's or organization's INFOSEC, IA, physical security, force protection, and so forth. This ensures the security programs do not provide conflicting guidance and work together to support each other.

3–3. Program awareness and training product promotion

a. Active promotion of the OPSEC program is the responsibility of commands. ACOMs, ASCCs, DRUs, and installations are encouraged to develop their own OPSEC training products and use all suitable techniques of publicity and promotion consistent with law and within funds available.

b. As part of promotional efforts, commanders/directors at all levels should-—

(1) Advertise the OPSEC program through posters, billboards, inserts in bulletins, or other media which frequently reach Soldiers, DA civilians, contractors, and Family members.

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

(3) Note that appropriated funds generally may *not* be used to purchase promotional items to be given away to government employees, members of the public, or others. Such expenditures can only be justified under very unusual and unique circumstances, and must always be reviewed by servicing legal counsel before any funds are obligated for such a purpose.

3–4. Threat analysis support to OPSEC

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

Chapter 4
Training Requirements

4–1. Overview

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

4–2. Training programs

Commanders and equivalent leadership positions will ensure all personnel receive appropriate level OPSEC training based on their duties or position.

a. OPSEC Level I certification training. The target audience for Level I is all personnel (which includes Soldiers, civilians, and contractors). Level I training is composed of both initial and continual awareness training.

(1) *Initial OPSEC awareness training.* All newly assigned personnel within the first 30 days of arrival in the organization (this includes accessions and initial entry programs) must receive initial training. It is recommended this training be conducted as part of an initial entry briefing or unit/organization newcomer's briefings. This training is provided by the unit or organization's OPSEC officer and can be conducted via distance learning, providing all necessary objectives are met. The intent and focus of initial training will be on the following areas:

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

(b) Understanding what constitutes critical information.

(c) Understanding how adversaries aggressively seek information on U.S. military capabilities, activities, limitations, intentions, and plans.

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

(e) The intended endstate is that each individual has the requisite knowledge to safeguard critical information and know the answers to the following questions:

1. What is my unit or organization's critical information?

2. What critical information am I personally responsible for protecting?

3. How is the threat trying to acquire my critical information?

4. What steps am I/are we taking to protect my/our critical information?

5. Who is my OPSEC officer (in order to report an OPSEC concern, compromise, or ask an OPSEC question)?

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

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

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

(c) OPSEC training specific to the relevant area of operations will be provided to deploying and redeploying personnel.

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

b. OPSEC Level II certification training. The HQDA OPSEC Officers Course will train and prepare personnel to manage an OPSEC program and advise the commander on all OPSEC matters. Graduates will have the requisite knowledge to effectively use OPSEC analytic techniques. This training will allow the OPSEC practitioner to identify vulnerabilities and select appropriate OPSEC measures to protect identified critical information. These acquired skills will assist the OPSEC Officer with planning and program development for overall program success and mission effectiveness. Individuals successfully completing the HQDA OPSEC Officer Course or IOSS equivalent will be qualified to provide Level I OPSEC training. The target audience for Level II training areas follows:

(1) OPSEC PMs and OPSEC officers are required to complete Level II training. Army personnel will attend the HQDA OPSEC Officers Course or the IOSS equivalent to be Level II certified. Personnel authorized or required to conduct OPSEC reviews from contract solicitation documents, and so forth, must also complete the OPSEC Level II certification.

(2) OPSEC coordinators, Web masters, PAOs, FOIA, speech writers, FRSAs, or any other personnel who interact with the public on a regular basis will receive external official presence (EOP) training or attend a Level II OPSEC officers course.

(3) OPSEC PMs/officers who have received OPSEC Level III certification training and maintain proficiency will be authorized to provide decentralized OPSEC Level II training to their commands, activities, installations, and organizations.

(4) The Army OSE will monitor the conduct of OPSEC Level II training to ensure standardization throughout the Army. While OPSEC Level II training will be decentralized, the OSE will centrally manage the certification of Level II and Level III OPSEC officers. OPSEC PMs/officers conducting OPSEC Level II training must coordinate with the Army OSE prior to providing this training.

c. OPSEC Level III certification training. The Army OSE offers Army Level III OPSEC instructor certification. OPSEC PMs at ACOMs, ASCCs, DRUs, corps, and installations may opt to receive OPSEC Level III training. This certification only applies to the HQDA OPSEC Officers Certification Course taught by the Army OSE as required by this regulation. The main roster of source documents for Level III certifications will be maintained by the Army OSE.

(1) Initial Level III OPSEC instructor certification requirements.

(a) Successfully completed the HQDA OPSEC Officers Course and be Level II certified.

(b) Meet the qualifications set forth in AR 530–1, H–6.

(c) Be recommended for Level III OPSEC instructor certification by a designated official in the grade of colonel/O–6, or equivalent (required for personnel not assigned at the ACOM/ASCC/DRU, corps, or installation level).

(d) Be familiar with the HQDA OPSEC Officers Course POI for course completion. POI can be obtained from the Army OSE.

(e) Be thoroughly familiar with the lesson plans for the entire OPSEC Officers Course curriculum. Lesson plans can be obtained from the Army OSE.

(f) Demonstrate knowledge of and ability to successfully teach at least two blocks of instruction each day of the OPSEC Officers Course with oversight from the OSE Level III certifier.

(g) Take and pass a 60-question, closed-book OPSEC Level III instructor examination, approved by the Army OSE, with at least an 80% score. Only one retest will be allowed.

(h) Obtain and maintain positive control of Level III certificates issued by the Army OSE.

(2) Level III OPSEC instructor maintenance requirements.

(a) Attend, when available and resources permit, at least one documented workshop or conference specifically pertaining to OPSEC annually.

(b) Maintain proficiency with the training curriculum to enhance OPSEC PM/officer skill-sets established by the Army OSE. Information can be obtained from the Army OSE.

(c) Provide complete and accurate class rosters with required information to the Army OSE within 30 days after completion of all Level II courses by uploading to the AKO OPSEC folder.

(d) Provide an after action report, critiques and test score sheets at the end of each course to the Army OSE within 30 days after completion of the course. Minimum information required for after action reports will be the number of students, identified by military/DA civilian/DoD, contractors, commands, and how many appointed OPSEC PMs/officers were in attendance and any anomalies that require changes.

(e) Maintain contact with the Army OSE for specific guidance and new updates.

(f) Provide at least two weeks in advance, the class dates, number of students, and name of instructors to the Army OSE for planning purposes.

(g) Level III instructors will ensure all students receive course materials.

(h) Level II classes are restricted to no more than 30 students. Waivers to increase class size must be approved by the Army OSE Chief.

(3) Auditing Level III OPSEC program manager/officer instructors.

(a) All active Level III certified instructors are subject to no-notice audits. The following must be accomplished by all Level III instructors to maintain certification status:

1. Assigned/appointed as an OPSEC PM/officer for an Army organization. If individual is no longer assigned duties as an OPSEC PM/officer, he/she will no longer be a certified Level III instructor unless recertified by the Chief, Army OSE.

2. Instructor for at least one Level II OPSEC PM/officer certification course class per fiscal year.

3. Maintain all requirements for initial Level III certification.

4. Must not delete any part or portion of the approved course curriculum; however, course materials may be added to, with OSE approval.

(b) Failure to meet or maintain any of the listed requirements may place the instructor in an inactive status. Once all requirements are satisfactorily met, the instructor certification can be reinstated by the Army OSE Chief. The Army OSE Chief will report the status of all active and inactive Level III instructors to the Army OPSEC Program Manager quarterly.

(c) DCS, G–3/5/7 (G–39) will provide funds for Army OSE to audit Level III instructors, as needed.

(4) Army OSE will—

(a) Ensure Level III instructors have the most current and up-to-date training materials.

(b) Provide guidance and recommendations in response to OPSEC queries/concerns/issues.

(c) Coordinate with Level III instructors for Army OSE periodic visits to audit the HQDA OPSEC Officers Course.

(d) Ensure Level III instructors receive any and all updated OPSEC all Army activities (ALARACTs) and other messages published by DCS, G–3/5/7 (G–39) or the Army OSE.

(e) Provide all signed course completion certificates for students.

(f) Maintain lines of communications with all Level III instructors and the Army OPSEC PM as it pertains to OPSEC, course materials, issues, and so forth.

(5) *Request for Level III Certification waiver*. Requests for ACOM, ASCC, DRU, corps, or installation-level waivers for Level III instructor nomination must be justified and forwarded through the Chief, Army OSE to the Army OPSEC PM for approval. Waiver requests must be accompanied by a recommendation from a colonel/O–6 or equivalent. Those requests not approved will be returned with appropriate justification back to the requestor.

4–3. OPSEC and external official presence training

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

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

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

4–4. Joint and interagency training

a. Joint OPSEC support element. The Joint OPSEC support element provides direct support to the Joint Staff, combatant commanders and Joint force commanders through integration of OPSEC into operational plans and exercises and by providing staff level program development and training and surveys/assessments, when directed.

b. Interagency OPSEC support staff. The IOSS supports the National OPSEC Program by providing tailored training, assisting in program development, producing multimedia products, and presenting conferences for the defense, security, intelligence, research and development, acquisition, and public safety communities. Its mission is to help government organizations develop their own, self-sufficient OPSEC programs in order to protect U.S. programs and activities. IOSS is recognized as the standard for government OPSEC programs and provides subject matter expertise to the Department of Defense.

(1) IOSS offers a multitude of OPSEC training aids which are available to all OPSEC officers (see https://www.iad.gov/ioss/index.cfm).

(2) Only adjunct faculty-certified personnel are able to conduct the DoD 2500 OPSEC Analyst and Program Management Course.

c. Joint OPSEC support element training. Army personnel are welcome and encouraged to receive training from the Joint OSE and/or IOSS. However, the training courses offered by the Joint OSE and IOSS provide a broader perspective of OPSEC for the Joint and interagency level while Army OPSEC training is oriented specifically to an Army audience.

d. Adjunct instructor. The IOSS uses the term “adjunct instructor” to identify those able to conduct the DoD 2500 OPSEC Analysis and Program Management Course. Personnel not assigned to the command levels in paragraph 4–2c, above, may also seek the OPSEC adjunct faculty certification but must submit a waiver through the chain of command to DCS, G–3/5/7 (G–39), justifying the need to be adjunct faculty-certified. The justification must be signed by an O–6/civilian equivalent or above. Certification for the 2500 course, as an alternative to the Army course, will be coordinated with the Army OSE at https://www.us.army.mil/suite/page/589183.

(1) To become certified, personnel must have successfully completed the DoD 2500 OPSEC Analysis and Program Management Course.

(2) The processes are much the same as the HQDA OPSEC Officer Course, such as instructing with a certified instructor, being critiqued by a certified instructor, and passing an exam.

(3) Successful completion of the IOSS requirements will certify the individual as an adjunct instructor for the DoD 2500 OPSEC Analysis and Program Management Course.

Chapter 5
Operations Security Review, Assessment, and Survey

Section I
Operations Security Review

5–1. General
The OPSEC review is a documented evaluation of information or visual products intended for public release to ensure protection of critical and/or sensitive information. Products that may require an OPSEC review can include, but are not limited to, memorandum letters, e-mail messages, articles, speeches, academic papers, videos, briefings, contractual documents, news releases, technical documents, proposals, plans, orders, response to FOIA requests, Privacy Act requests, and other visuals or electronic media. An OPSEC Level II-trained OPSEC officer may conduct an OPSEC review of products and provide mandatory guidance, as needed, prior to release in the public domain or to EOPs. This review is for information related to U.S. Government or military operations and other supporting programs prior to release to public domain for EOPs. An OPSEC review must be conducted in conjunction with a public affairs review for the release of official information to the public. The OPSEC review of a product is unrelated to the annual OPSEC program review. The results of the review must be documented and justifications annotated based on existing laws, EOs, DOD directives, instructions, Army Regulations, and internal policy, as well as individual CILs.

5–2. Procedures
a. SOP/OPSEC plans will state which products automatically go to the OPSEC officer for a review.

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

(2) News releases, Web content, and responses to FOIA and Privacy Act requests are examples of products that require automatic review by a public affairs-qualified NCO/DA civilian/officer or OPSEC officer.

(3) The specifics about whom and how these reviews are conducted need to be outlined in the organization's SOP/plan.

b. The OPSEC review may identify additional requirements (for example, corrective action, revision/removal of critical and/or sensitive information found in the product information and/or review by other functional areas like intelligence and information security reviews).

(1) When critical and/or sensitive information is found, corrective action will be recommended to the appropriate official in writing. OPSEC review data will be included in the annual OPSEC report.

(2) If the information requires official review beyond what the local OPSEC officer can provide (e.g., FOIA, intelligence, foreign disclosure, information security, other or non-DoD agency information, etc.), the OPSEC officer will forward the matter with a written request for such review to the appropriate official or officials.

c. Technical papers and reports must contain distribution statements according to AR 25–30, AR 70–1, AR 70–31, DoDI 5230.24, and DoDD 5230.25. This includes contractors producing technical information for the U.S. Government.

d. In accordance with AR 25–1 and AR 25–2, sensitive information may not be placed on a Web site that is accessible to the public.

(1) All official, publicly accessible, organizational Web sites must have an OPSEC Web site review to ensure no operationally sensitive and/or critical information is posted to or contained thereon, as per AR 25–1 and AR 25–2.

(2) The OPSEC Web site review is the responsibility of the Webmaster/maintainer, in coordination with the OPSEC officer, PAO, and other appropriate designees (to include, but not limited to, security, intelligence, and legal personnel).

(3) Information not authorized for release to the public on any Web site is also not releasable in any other public forum. Official Web sites must be in compliance with all applicable Army and DoD guidance and policies.

e. The unit CIL approved by the commander, in addition to restrictions stated in subparas *b*, *c*, and *d*, above, provides a basis for determining releasability.

Section II
Operations Security Assessment

5–3. General
The OPSEC assessment is an evaluative process, conducted annually of an organization, operation, activity, exercise, or support function to determine if sufficient OPSEC measures are in place to protect critical information. An OPSEC

program assessment may include self assessments, program reviews as part of inspector general inspections, or higher headquarters assessments specifically addressing OPSEC. The OPSEC assessment determines the overall OPSEC posture and degree of compliance by the assessed organization with applicable OPSEC plans and programs. The OPSEC assessment team should be composed of the OPSEC PM/OPSEC officer and appropriate subject matter experts from throughout the organization.

5–4. Procedures

a. Each OPSEC PM/officer will conduct an annual self assessment to determine the effectiveness of his or her OPSEC program, and as a minimum, assess the status of the following:

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

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

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

(4) The status of OPSEC training.

b. At each command level, the organization must conduct an OPSEC assessment of subordinate units using the published OPSEC guidance to determine if the unit being assessed is implementing higher headquarters-directed and their own OPSEC policies and procedures. The command OPSEC officer submits a written assessment with results and recommendations to the assessed unit commander or commander that directed the assessment. As a minimum, the following will be assessed:

(1) Identification of critical information.

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

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

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

(5) The status of OPSEC training.

(6) Application of a formal OPSEC checklist based on restrictions in existing laws, statutes, regulation and policy, including any specific requirements applicable only to the assessed organization and/or other organizations of its type.

(a) The higher headquarters must develop and publish an OPSEC checklist (or checklists, if differing OPSEC requirements apply to different subordinate organizations) as part of the organizational inspection program (OIP)/ command inspection program (CIP).

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

Section III
Operations Security Survey

5–5. General

a. A survey is the application of the OPSEC methodology by a team of experts to conduct a detailed analysis of activities associated with a specific organization, operation, activity, exercise, or support function by employing the known collection capabilities of potential adversaries. This evaluation should focus on the agency's ability to adequately protect critical information from adversary intelligence exploitation during planning, preparation, execution, and post-execution phases of any operation or program. Surveys must be conducted every three years or as requested by the commander or higher headquarters.

b. OPSEC surveys are personnel, resource, and time-intensive and should only be conducted as triennially required (per the preceding paragraph) or when deemed necessary by the commander. Extremely sensitive programs, activities, or operations where the slightest compromise will result in mission failure and/or extreme damage to national security are rare examples of where additional OPSEC surveys (i.e., in addition to the required triennial survey) are more likely to be warranted.

c. Activities that warrant additional OPSEC surveys include, but are not limited to, RDT&E, acquisitions, treaty verification, nonproliferation protocols, international agreements, force protection operations, special assess programs, and activities that prepare, sustain, or employ U.S. Military Forces over the range of military operations.

5–6. Procedures

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

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

c. The OPSEC surveys vary according to the nature of the information, the adversary collection capability, and the environment. In combat, surveys identify weaknesses which can endanger ongoing and impending combat operations.

In peacetime, surveys assist in correcting weaknesses which disclose information useful to adversaries in future conflict, or in compromising ongoing research and development programs and activities.

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

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

(2) 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. Additionally, if the survey is conducted by the Army OSE, a report is provided to the requesting commander.

e. There are two types of surveys—

(1) A command survey concentrates on events that 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 organizational lines with prior coordination.) The survey team includes members from both inside and outside the surveyed organization. A letter or message initiates the formal survey. It states the subject, team members, and dates of the survey. It can also list organizations, activities, and locations. Contact the Army OSE for more information.

Chapter 6
Operations Security Contractual Documents Review Requirements

6–1. Overview

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

6–2. Policy and procedures

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

b. For unclassified contracts, the RA OPSEC officer will review contractual documents to determine if any specific OPSEC measures are required in a contract. The RA OPSEC officer will integrate any needed OPSEC measures into the PWS, the statement of work (SOW), or the statement of objectives (SOO) in sufficient detail to ensure complete contractor understanding of the exact OPSEC measures required by the RA. The government contracting activity will integrate the OPSEC measures into the solicitation package and resultant contract, based on the RA's coordination using the AT/OPSEC Desk Reference cover sheet. If the contract is modified or given another option year, this review process will be repeated to ensure required OPSEC measures remain current and relevant throughout the lifecycle of the contract.

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

d. For classified contracts, the RA OPSEC officer will coordinate with the RA's industrial security specialist. If the RA does not have an industrial security specialist, the RA will coordinate through their chain of command for an industrial security specialist or submit a request to an appropriate outside agency for industrial security support for completion of a DD Form 254 (Department of Defense Contract Security Classification Specification). The industrial

security specialist completes the DD Form 254 which is used to convey security requirements in a classified contract. Contractor input is encouraged but is not required. The industrial security specialist will review the SOW, SOO, or PWS to ensure the appropriate security clauses and/or language are contained therein to address the protection of classified information. The industrial security specialist ensures the OPSEC measures contained in the SOW, SOO, or PWS are also reflected on the DD Form 254. The industrial security specialist will forward the fully executed DD Form 254 to the RA for submission to the government contracting activity. If the contract is modified or given another option year, this process will be repeated to ensure the DD Form 254 remains current and relevant throughout the lifecycle of the contract.

Chapter 7
Special Access Programs

7–1. Overview

a. A Special Access Program (SAP) is a security program established under EO 13526 and authorized by the Secretary of Defense to administer extraordinary security measures to control access and provide protection of extremely sensitive information in addition to the provisions of AR 380–5 for classified information. The SAP manager, director, or commander is responsible for OPSEC for the SAP.

b. AR 380–381 and DoDI 5205.11, Management, Administration, and Oversight of DoD SAPs and the DoD Overprint to the National Industrial Security Program Operating Manual (NISPOM) Supplement prescribe policies and procedures for establishing, administratively controlling, supporting, and decertifying SAPs.

7–2. Policy

Each SAP will have a functioning OPSEC program with an appointed OPSEC officer from conception to disestablishment. The SAP OPSEC program will use the process described in chapter 3 of this regulation 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 a*s a part of the PPP.

a. The DCS, G–3/5/7, in coordination with the DCS, G–2 and Army Special Programs Directorate, will provide policy guidance and HQDA staff oversight for SAP OPSEC procedures.

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

c. The SAP OPSEC officer will comply with the provisions of chapter 3 of this regulation and AR 380–38l. The SAP OPSEC officer will manage and document the SAP's OPSEC program. The SAP OPSEC officer is the liaison between the SAP and the command for OPSEC issues. Due to stringent SAP security measures, the command OPSEC program manager or unit/organization OPSEC officer may not always have knowledge of the SAP.

Appendix A
References

Section I
Required Publications

AR 1–201
Army Inspection Policy (Cited in para 2–8e.)

AR 25–1
Army Information Technology (Cited in paras 2–18a(15)(a), 2–18a(15)(b), 4–3b, 5–2d, 5–2d(1), G–3a.)

AR 25–2
Information Assurance (Cited in paras 5–2d, 5–2d(1), G–3a, G–3a, G–3c.)

AR 25–55
The Department of the Army Freedom of Information Act Program (Cited in para L–2.)

AR 380–5
Department of the Army Information Security Program (Cited in paras 2–1f(2), 2–1I, 2–18a(14), 7–1a, G–2b, L–2.)

AR 381–12
Threat Awareness and Reporting Program (Cited in para 2–22k.)

DODD 5205.02E
DOD Operations Security Program (Cited in paras 1–5a(1), 1–6a.)

Section II
Related Publications
A related publication is a source of additional information. The user does not have to read it to understand this regulation.

AR 25–30
The Army Publishing 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 350–1
Army Training and Leader Development

AR 360–1
The Army Public Affairs Program

AR 380–27
Control of Compromising Emanations

AR 380–40
Safeguarding and Controlling Communications Security Material (U)

AR 380–49
Industrial Security Program

AR 380–53
Communications Security Monitoring

AR 380–381 (U)
Special Access Programs (SAPs) and Sensitive Activities

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

AR 525–21 (S)
Military Deception (U)

DoDD 3020.40
DoD Policy and Responsibilities for Critical Infrastructure

DoDD 5000.01
The Defense Acquisition System

DoDD 5230.25
Withholding of Unclassified Technical Data from Public Disclosure

DoDD 5400.07
DOD Freedom of Information Act Program

DoDI 5000.02
Operation of the Defense Acquisition System

DoDI 5200.39
Critical Program Information Protection (CPI) within the Department of Defense

DoDI 5205.11
Management, Administration, and Oversight of DoD Special Access Programs (SAPs)

DoDI 5230.24
Distribution Statements on Technical Documents

DoDM 3020.45–M–V3
Defense Critical Infrastructure Program (DCIP) Security Classification Manual (SCM)

DoDM 5200.01
DoD Information Security Program

DoDM 5205.02–M
DoD Operations Security (OPSEC) Program Manual

Executive Order 13222
Continuation of Export Control Regulation

EO 13526
Classified National Security Information

Joint Publication 2–0
Joint Intelligence

Joint Publication 3–13
Operations Security

National Security Decision Directive 298
National Operations Security Program

National Telecommunications and Information Systems Security Directive (NTISSD) No. 600
Communications Security Monitoring (Available at http://www.iad.nsa.smil.mil/resources/library/cnss_section/pdf/nstissd_600.pdf.)

UCMJ, Article 92
Failure to Obey Order or Regulation

15 CFR 730.1–774.2
Export Administration Regulations

15 CFR 768.1 et seq.
Foreign Availability Determination Procedures and Criteria

22 CFR 120.1–130.17
International Traffic in Arms Regulations

5 USC 552
Public information; agency rules, opinions, orders, records, and proceedings

5 USC 552a
Records maintained on individuals

10 USC 3013
Secretary of the Army

50 USC App. 2401–2420
Export Regulation

50 USC 1701–1707
International Emergency Economic Powers

131 S. Ct. 1259 (2011)
Milner v. Department of the Navy

Section III
Prescribed Forms
This section contains no entries.

Section IV
Referenced Forms
Unless otherwise indicated, DA forms are available on the Army Publishing Directorate (APD) Web site (www.apd.army.mil/); DD forms are available on the Office of the Secretary of Defense (OSD) Web site (www.dtic.mil/whs/directives/infomgt/forms/index.htm/).

DA Form 11–2
Internal Control Evaluation Certification

DA Form 2028
Recommended Changes to Publications and Blank Forms

DD Form 254
Department of Defense Contract Security Classification Specification

Appendix B
The Operations Security Process

B–1. Overview
The OPSEC process consists of five steps which can apply to any plan, operation, program, project, or activity. These steps provide a framework for the systematic process necessary to identify, analyze, and protect sensitive information.

The process is continuous and assessments should occur frequently throughout an operation. It considers the changing nature of critical information, the threat, and vulnerability assessments throughout the operation. It uses the following steps:

a. Identification of critical information.

b. Analysis of threats.

c. Analysis of vulnerabilities.

d. Assessment of risk.

e. Application of OPSEC measures.

B–2. Identification of critical information

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

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

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

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

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

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

b. There are several sources which can help the OPSEC officer determine the unit or organization's critical information.

(1) The supporting intelligence element will provide information on the adversary and its intelligence requirements. Known tasking of the adversary's intelligence system for answers to specific questions about friendly intentions, capabilities, limitations, and activities will be part of critical information.

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

(3) The commander, director, or equivalent leadership position will provide specific guidance.

(4) The security classification guide for a program or operation identifies classified critical information. The security classification guide itself identifies the most sensitive areas of an activity, program, project, or operation.

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

(a) Information concerning a protected person.

(b) Export-controlled technical data (on the Military Critical Technologies List, as required by the Export Administration Act (50 USC App. 2401–2420), extended by EO 13222 under the International Emergency Economic Powers Act (50 USC 1701–1707)).

(c) Critical information.

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

(e) Military operational and tactical information.

(f) DoD-developed computer software.

(g) Proprietary data (trade secrets).

(h) Test materials used in an academic environment.

(i) Law enforcement sensitive information.

(j) Personally identifiable information.

(6) Appendix C has sample critical information by category of information.

(7) Indicators that would reveal critical information are also critical information. Appendix D has samples of OPSEC indicators that could reveal critical information.

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

d. The commander must approve the organization's critical information and abide by critical information provided by the higher element or commander.

B–3. Analysis of threats

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

b. Methodology.

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

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

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

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

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

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

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

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

(e) Which indicators can be used to friendly advantage by fostering a desired perception by the adversary that will be beneficial to friendly operations? (Coordinate with military deception (MILDEC) planners and military information support operations officers.)

B–4. Analysis of vulnerabilities

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

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

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

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

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

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

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

d. If required, refer to AR 525–21(C) for information on deception, and refer to AR 381–102 (S) for information on cover.

e. Appendix F has sample OPSEC measures.

B–5. Assessment of risk

The purpose of this step is to select which of the tentative OPSEC measures to implement. The OPSEC PM/officer recommends to the commander the OPSEC measures that he or she believes should be implemented, but the

commander responsible for the mission must make this decision. The commander must balance the risk of operational failure against the cost of OPSEC measures.

a. Consider the following questions for each tentative measure. The PM/officer must be prepared to answer each of these questions for the commander.

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

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

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

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

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

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

c. Check the interaction of OPSEC measures. Ensure that a measure to protect a specific piece of critical information does not unwittingly provide an indicator of another.

d. Determine the coordination requirements for OPSEC measures with the other capabilities.

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

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

B–6. Application of appropriate operations security measures

a. The purpose of this step is to apply OPSEC measures, approved by the commander, to ongoing activities or to incorporate them into plans for future operations. There are two aspects to this step-the PM/officer implements the OPSEC measures and then, unit personnel implement the OPSEC measures.

(1) The PM/officer implements OPSEC measures. The OPSEC officer can implement OPSEC measures by generating guidance or tasking. The guidance or tasking can be in the form of annexes to plans, OPSEC plans, SOPs, and memoranda which may be issued in hard copy or by electronically-transmitted messages. The OPSEC officer will—

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

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

(c) Appendix N has a sample format for an OPSEC annex or appendix. This format may be used in support of all activities and operations, in addition to information operations.

(d) There is no set format for an OPSEC plan. Appendix O 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 the identification and protection of critical information from initial planning through post-execution phases.

2. Tasks to staff and subordinate commands to plan and execute OPSEC measures.

3. An OPSEC estimate comprising the identified or assumed adversary knowledge of friendly operations or activity, friendly critical information, and an evaluation of friendly OPSEC effectiveness.

4. Intelligence collection threat consisting of friendly detectable indicators, critical information, and the adversary's capability to obtain and use the 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.

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

b. After the implementation of appropriate measures, the OPSEC PM/officer should evaluate the effectiveness of OPSEC measures during execution.

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

(2) As part of the OPSEC evaluation process, the OPSEC program manager/officer will—

(a) Evaluate the effectiveness of current OPSEC measures.

(b) Provide emphasis when needed.

(c) Recommend adjustments to improve the effectiveness of existing measures.
(d) Recommend new measures, if significant new vulnerabilities develop.

B–7. Planning guidance

a. OPSEC steps occur within the military decisionmaking process. The OPSEC officer provides planning guidance for staff elements. Each staff element will identify the critical information, who is responsible for protecting it, and the vulnerabilities in their functional areas, and provide them to the OPSEC officer.

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

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

(2) A preliminary list of critical information.

(3) A summary of adversary intelligence collection capabilities.

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

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

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

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

Appendix C
Sample Critical Information

C–1. Overview

The following paragraphs provide a few examples of critical information. There are many other items of critical information 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 critical information unique to itself.

C–2. Courses of action

a. Specific courses of action (COA) the U.S. and allied commands are planning.

b. Specific COA that U.S. and allied forces cannot undertake or execute.

C–3. Forces

a. U.S. and allied forces earmarked for possible COA.

b. Readiness levels of organizations.

c. Specific current force/unit locations.

d. Specific projected force/unit locations.

C–4. Mission command

a. U.S. and allied command arrangements for executing COA.

b. Current or future locations of unit commanders.

c. Current or future command post locations.

d. Command post vulnerabilities.

C–5. Communications

a. Command, control, communications, computers, and intelligence capabilities.

b. Communications sites locations.

c. Communications limitations (weather, terrain and equipment shortages, and so forth).

C–6. Logistics

a. Logistical posture of U.S. and allied forces.

b. Speed of deployment/redeployment of ground and air forces.

c. Pertinent ground, air, and sea lines of communications; locations of storage depots, ports, and airfields.

d. Vulnerabilities to interdiction of the lines of communication.

e. Contents of Army prepositioned stocks and significant restructuring of Army prepositioned stocks.

C–7. Supplies

a. Levels of supplies available for immediate support.
b. Pre-positioned supply sites.
c. Period of combat sustainment with those supplies.
d. Critical item shortages (in all classes).
e. Limitations to resupply capability.
f. Demand level for Class IX items.

C–8. Locations

a. Specific locations of exercises and operations.
b. Specific locations of participating forces.
c. Specific projected force/unit locations.
d. Alternate force/unit locations.

C–9. Vulnerabilities

a. Vulnerabilities of defensive dispositions.
b. Vulnerabilities of sensors and other capabilities to detect attack.
c. Vulnerabilities to attack.
d. Vulnerabilities of units and weapons and weapons systems.
e. Vulnerabilities in protection or security forces or security plans.

C–10. Intelligence

a. Intelligence, surveillance, and reconnaissance (ISR) resources available to support the commander.
b. Locations of those ISR capabilities.
c. Ongoing ISR operations and their goals.
d. Vulnerabilities to exploitation or destruction of those friendly ISR capabilities.

C–11. Rules of engagement

Policies and rules of engagement that govern the use of weapons and electronic or acoustic warfare systems.

C–12. Allies

a. Nations providing current or future support to the United States.
b. Vulnerabilities that could be exploited to reduce or eliminate such support.

C–13. Maintenance

a. Maintenance and salvage capabilities of the United States and allied forces.
b. To what degree these capabilities can support and sustain forces in combat.
c. Vulnerabilities to attack.

C–14. Weapons

a. Specific characteristics and capabilities of weapons and electronic systems available to coalition forces.
b. Doctrine for using various weapons.
c. Indicators that unconventional weapons will be employed.
d. New weapons that are available or are being employed.
e. Vulnerabilities and limitations in friendly weapons and weapons systems.

C–15. Military Information Support Operations

a. Intended psychological warfare and subversion operations.
b. Plans to exploit adversary vulnerabilities.
c. Ongoing operations.
d. U.S. agencies conducting operations.
e. Military information support operations themes and objectives.
f. Vulnerabilities of U.S. forces to psychological warfare and subversion.

C–16. Special operations forces and unconventional warfare

a. Intended sabotage and direct action mission targets.
b. Adversary vulnerabilities planned for exploitation.
c. Friendly capabilities to conduct unconventional warfare operations.

d. U.S. agencies controlling those resources.
e. Special operations forces (SOF) team deployment dates.
f. SOF team deployment sites.
g. Number of SOF teams/personnel in an area.
h. Indigenous support to SOF teams.
i. Conventional units associated with SOF teams/personnel.

C–17. Deception

a. Planned political and military deceptions.
b. Ongoing deception operations.
c. U.S. agencies conducting deception operations.
d. Identity of military units/organization conducting or participating in deception activities.

C–18. Deception vulnerabilities

Vulnerabilities of U.S. commanders and staffs to deception.

C–19. Counterintelligence

a. U.S. counterintelligence capabilities to detect and neutralize espionage and sabotage nets.
b. Number of CI assets available.
c. Identification and location of CI elements and activities.
d. Identification of local personnel that may be assisting friendly CI forces.

C–20. Research, development, test and evaluation programs

a. Weapons systems development schedules (dates, times, locations).
b. Emerging technologies, tactics, techniques, and procedures applicable to new weapons systems/equipment.
c. Computer software used in weapons systems development, testing and evaluation.
d. Location of unclassified computer data bases used by the RDT&E community.
e. Specific contract criteria stated in a classified contract.
f. Identification of special access elements within a contract or program.
g. Specific PPP implementation methods.

C–21. Medical

a. Casualty figures, both actual and projected.
b. Very Important Persons (VIP) being treated by our medical treatment facilities.
c. Overall bed/treatment capacity.
d. Increased medical supplies (vaccines, blood products, and so forth) required by unit or theater.
e. Shortages in medical military occupational specialties and personnel.
f. Identification of projected medical personnel/team deployments.
g. Specific identification of classified medical-related research programs.
h. Identified medical vulnerabilities of friendly forces.

C–22. Systems acquisition

a. Corporations or companies projected to be involved in system acquisition.
b. Funding amounts of the acquisition program.
c. Specifics or requirements of the program in acquisition.
d. Classification levels of the program.
e. Duration of the acquisition.
f. Shortfalls in ability to conduct an acquisition on time to meet requirement.

C–23. Government contractors

a. Programs in which the contractor provides classified services and support to the U.S. Government.
b. Pre-contract award identification of locations of contractor duty.
c. Contractor increasing hiring for new or existing contracts or programs.
d. Contractor information or service-sharing agreements with other private organizations.

C–24. Arms Control Treaty inspections

a. Missions of the activities on the installations to be visited.

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

c. If all the buildings on the installation are in use.

d. Access to the post.

e. Morale of installation personnel.

f. Condition of the installation.

g. Portions of the installation that appear to have more protection/security than other parts of the installation.

h. Security procedures in place at this installation (Federal Bureau of Investigation support, physical security, counterintelligence activities, law enforcement).

C–25. Automated Information Systems

a. AIS protection being implemented (measures/procedures).

b. AIS approvals/certifications.

c. Type of AIS equipment protection within an office environment and/or remote site.

d. Specific identified vulnerabilities in AIS protections at specific locations.

C–26. Special access programs

a. Organizations and contractors involved in the SAP.

b. Mission or subject of the SAP.

c. Operational life of the SAP/current stage of development.

d. Security procedures for the SAP.

e. Budget for the SAP.

f. Number of personnel in the SAP.

g. Existence and identification of an unacknowledged SAP.

C–27. Cyberspace

a. Wireless communication.

b. Computer network defense.

Appendix D
Operations Security Indicators

D–1. Characteristics

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

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

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

when intelligence detects the headquarters company and one line company. When taken as a whole, the pattern can be a single indicator, which simplifies the adversary's problem.

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

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

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

D–2. Sample operations security indicators

The following are 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.

D–3. Administration

a. Temporary duty 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 and International Civil Aviation Organization notices.
l. Change of mail addresses or arrangements to forward mail on a large scale.
m. Runs on post exchange for personal articles, for example, to include personal radios.
n. Emergency personnel requisitions and fills for critical skills.
o. Emergency recall of personnel on leave and pass.

D–4. Operations, plans, and training

a. Changes in defense readiness condition, force protection condition, or information condition.
b. Movement of forces into position for operations.
c. Abnormal dispersions or concentrations of forces.
d. Deviations from routine training.
e. Rehearsals and drills for a particular mission.
f. Exercises and training in particular areas with particular forces.
g. Repeating operations the same way, same time, same route, or in same area. Fixed schedules and routes.
h. Standard reactions to hostile acts.
i. Standardizing maneuvers or procedures.
j. Standardizing force mixes and numbers to execute particular missions down to squad-level operations.
k. Changing guards at fixed times.
l. Appearance of special purpose units (bridge companies, pathfinders, explosive ordnance detachments, SOF, liaison officer teams, and so forth).

m. Change in task organization or arrival of new attachments.
n. Artillery registration in new objective area.
o. Surge in food deliveries to planning staffs at major headquarters.
p. Unit and equipment deployments from normal bases.

D–5. Communications

a. Voice and data (telephone, cellular phone, wireless) transmissions between participants in an operation.
b. Establishment of command nets.
c. Changes in message volume (phone calls to secure systems), such as increased radio, e-mail, and telephone traffic from headquarters.
d. Units reporting to new commanders.
e. Identification of units, tasks, or locations in unsecured transmissions.
f. Increased communications checks between units/organizations.
g. Unnecessary or unusual increase in reporting requirements.
h. Sudden imposition of communications security measures, such as radio silence.
i. Appearance of new radio stations in a net.
j. Communications exercises.
k. Appearance of different cryptographic equipment or materials.
l. Increase in unofficial use of commercial e-mail services.
m. Unofficial use of instant messenger and chat forums.
n. Increased FRG/FRSA posture.

D–6. Intelligence, counterintelligence, and security

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

D–7. Logistics

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

D–8. Engineer

a. New facility leases.

b. Construction of mock-ups for special training.
c. Production or requisitions of unusual amounts of maps and charts or products for unusual areas.
d. Attachment of specialized heavy equipment.

D–9. Medical

a. Stockpiling plasma and medical supplies.
b. Movement of deployable medical sets.
c. Immunization of units with area-specific and time-dependent vaccines.
d. Identifying special medical personnel and teams deploying to specific areas.
e. Sudden recall of Army National Guard and Army Reserve doctors to active duty.

D–10. Emissions other than communications

a. Radar and navigational aids that reveal location or identity.
b. Normal lighting in a blackout area.
c. Operating at unusual speed in water.
d. Loud vehicle or personnel movements.
e. Smoke and other odors.

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

a. Solicitations for subcontractors to perform portions of the work.
b. Lists of installations that are involved in particular contracts or projects.
c. Specialized hiring of personnel for particular contracts or projects.
d. Highlighting specific security needs or requirements for portions of a projector contract.
e. Testing range schedules.
f. Unencrypted emissions during tests and exercises.
g. Public media, particularly technical journals.
h. Budget data that provides insight into the objectives and scope of a system research and development 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 E
The Threat

E–1. Overview

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

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

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

(3) Catastrophic threats involve the acquisition, possession, and use of weapons of mass destruction or methods producing effects of weapons of mass destruction.

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

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

c. The asymmetric methods of warfare involve a strong emphasis on collecting information from unclassified and open sources. Because the U.S. is a free and open society, information is readily available and easy to access. Adversaries are exploiting this vulnerability by aggressively reading open source and unclassified material about the U.S. Army. As a result, many adversaries do not need to invest in costly and highly technical intelligence collection systems when they can obtain as much as 80% of the information they are seeking openly and legally.

E–2. Adversaries

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

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

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

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

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

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

E–3. Threat collection in the basic intelligence disciplines

Intelligence disciplines are categories of intelligence functions. The Army's intelligence functions are all-source intelligence, human intelligence (HUMINT), imagery intelligence (IMINT), signals intelligence (SIGINT), measurement and signature intelligence (MASINT), technical intelligence (TECHINT), and CI. Although Joint Publication (JP) 2–0 defines these intelligence disciplines, it also includes open source intelligence (OSINT) as a separate intelligence discipline. Because OSINT is more appropriately defined as a category of information, used singularly or integrated into an all-source analytical approach, it is not defined in Army doctrine as an intelligence discipline.

a. All-source intelligence.

(1) All-source intelligence is a separate intelligence discipline that is defined as the intelligence products, organizations, and activities that incorporate all sources of information and intelligence, including open source information, in the production of intelligence. Adversaries seek information from all available sources and will consolidate them into all-source intelligence products.

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

(a) OSINT involves the collection and analysis of freely available information, such as that presented in the media or available in libraries or the Internet. Open source information includes photographs, newspapers, magazine advertisements, government and trade publications, contract specifications, congressional hearings, computers, and other public media. Up to 80 percent of the adversary's intelligence needs can be satisfied through access to open sources without risk and at minimum cost.

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

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

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

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

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

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

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

(c) Greed, unexplained financial gain, alcoholism, drug abuse, sexual misconduct, marital infidelity, and financial indebtedness are among the human vulnerabilities exploited by threat HUMINT collectors. Disenchanted idealists are also a fertile source of information. Another recruitment technique involves misrepresentation of status or the "false flag" approach. A threat agent will attempt to pass himself off as an agent of a U.S. agency or of a friendly government to solicit cooperation.

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

(1) The most serious threat at the strategic level stems from 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 enhance the quality and timeliness of the intelligence product for our adversaries.

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

d. Signals intelligence. SIGINT incorporates the sub-disciplines of communications intelligence (COMINT) electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT).

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

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

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

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

f. Technical intelligence.

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

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

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

E–4. Technology transfer

a. 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 of 1979, (50 USC App. §§ 2401–2420), extended by EO 13222 under the International Emergency Economic Powers Act (50 USC §§ 1701–1707) and renewed through at least August 17, 2014 (see Presidential declaration at 78 Fed. Reg. 49107), addresses this threat by emphasizing the control of critical technology. To accomplish this task, DoD has enacted a series of initiatives to protect U.S. critical technologies. 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 DoDD 5000.01 and DoDI 5000.02. The following serves to outline the threat which exists in the illegal transfer of U.S. Government technology:

(1) The threat is actually many threats from many external sources, both governmental and commercial (often working together).

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

(3) 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.

(4) 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.

b. The Export Administration Act of 1979 is subject to an annual renewal requirement. Be sure to check whether the Act has been renewed.

Appendix F
Sample Operations Security Measures

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

F–1. Operations and logistics

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

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

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

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

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

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

g. Use darkness to mask deployments or force generation.

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

i. Randomize convoy routes, departure times, speeds, and so forth.

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

k. Do not use same landing zone or pick-up point repetitively.

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

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

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

F–2. Technical

a. Use radio communications emission control, low probability of intercept techniques, traffic flow security, ultra high frequency relay via aircraft, burst transmission technologies, secure phones, landline, and couriers. Limit use of high frequency radios and directional super high frequency transponders.

b. Control radar emissions and operate at reduced power.

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

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

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

f. Use deceptive radio transmissions.

g. Use decoy radio or emission sites.

F–3. Administrative

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

b. Conceal budgetary transactions, supply requests and actions, and arrangements for services that reveal preparations for 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. Destroy (burn, shred, and so forth) paper to include unclassified information to prevent the inadvertent disposal of classified and sensitive information.

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

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

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

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

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

F–4. Military deception

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

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

F–5. Combat action

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

Appendix G
Operations and Security Relationships to Security Programs

G–1. Background

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

G–2. Information security

a. INFOSEC is the system of policies, procedures, and requirements established under the authority of EO 13526, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

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

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

G–3. Information assurance

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

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

c. IA is the security discipline that encompasses communications security (COMSEC), computer security, and emanations security. See AR 380–40, AR 380–27, and AR 25–2.

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

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

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

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

(3) Emanations security is the component of COMSEC that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. In emissions security, TEMPEST refers to investigations and studies of compromising emanations.

G–4. Electronic security

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

G–5. Emanation control

Emanation control is the selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities, while minimizing, for OPSEC—

a. Detection by enemy sensors.

b. Mutual interference among friendly systems.

c. Enemy interference with the ability to execute a MILDEC plan.

G–6. Military deception

MILDEC supports military operations through the application of techniques that simultaneously deny certain true information or indicators and convey or display false information or indicators that will be accepted by adversaries. MILDEC actions mislead adversaries, causing them to derive and accept desired appreciations of U.S. military capabilities, intentions, operations, and other activities.

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

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

G–7. Physical security

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

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

b. OPSEC can support physical security by identifying those actions and information that would be indicators an adversary could exploit.

G–8. Force protection

Force protection consists of actions taken to prevent or mitigate hostile actions against all DoD personnel (Service members, civilians, DoD contractors, and Family members), resources, facilities, and critical information. Force protection does not include actions to defeat the adversary or protect against accidents, weather, or disease. OPSEC plays a vital role in the following ways:

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

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

c. OPSEC can identify indicators and recommend OPSEC measures to protect possible or existing vulnerabilities in protective measures.

d. OPSEC can assist traditional security disciplines in ensuring their protective measures are in the right place at the right time.

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

G–9. Program protection planning

a. DoDI 5200.39 identifies the requirements for PPP. This directive specifies CPI (the focus of program protection planning) shall be identified early in the acquisition life cycle, but not later than Milestone B, or when the program enters the acquisition process. It also states that, if CPI is identified, then a PPP is required. DoDI 5200.39 does not allow for waivers or exceptions to this requirement. If no CPI is identified, a PPP is not required.

b. DoDI 5200.39 references DoDM 5200.01 as a procedural manual for the development and implementation of PPPs. The PPP uses security disciplines and OPSEC to achieve protection.

Appendix H
Standard Duty Description for Operations Security Program Managers, Officers, and Coordinators

H–1. Overview

This section discusses the three positions of the OPSEC program.

H–2. General operations security duties

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

b. Identify the organization's critical information, recommend the CIL to the commander for approval, and publish the CIL.

c. Publish an OPSEC SOP/plan per guidance of this regulation. Ensure the OPSEC SOP/plan conforms to guidance from higher headquarters and any applicable local authorities, such as the installation OPSEC PM.

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

e. Conduct OPSEC reviews per guidance of this regulation.

H–3. Operations security program manager duties

The organization's OPSEC PM administers the commander's OPSEC program. An OPSEC PM is responsible for the development, organization, and administration of an OPSEC program at ACOM, ASCC, DRU, garrison, and corps and higher. The OPSEC PM provides guidance and oversight to multiple subordinate OPSEC programs of various units, activities, and organizations, and coordinates their actions under the command's OPSEC program. OPSEC PMs are also OPSEC officers, but because of the extent and complexity of the OPSEC program they oversee, they are primarily referred to as OPSEC PMs. In addition to H–2, above, OPSEC PMs —

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

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

c. Oversee all OPSEC training requirements.

d. Establish OPSEC as an element of the CIP.

e. Conduct OPSEC assessments of their own organization and subordinate elements.

f. Interface with all subordinate OPSEC officers and coordinators on issues that affect the command.

g. Interface and conduct OPSEC coordination with all higher headquarters.

h. For ACOMs, ASCCs, and DRUs, submit the annual OPSEC report to the Army OPSEC PM.

i. Maintain contact with Army protection personnel and security agencies to obtain information that supports the OPSEC planning process.

j. Ensure OPSEC is included in planning for future operations, exercises, tests, and activities. As required, write OPSEC documents, annexes, and appendices to OPLANSs and OPORDs. Write OPSEC documents as required for activities not covered by OPLANs and OPORDs.

k. Organize and provide oversight to an OPSEC working group. An OPSEC working group brings together OPSEC officers and other security-related positions to ensure the OPSEC program is consistent across the organization and is integrated at the work level. The working group will assist the OPSEC PM in developing OPSEC measures and solutions to implementation problems. The working group will provide coordination of all recommendations being forwarded to senior leadership and will assist with development of briefings and reports.

l. Interface with acquisition managers so that OPSEC is addressed throughout the lifecycle of any acquisition program.

H–4. Operations security officer duties

The OPSEC officer is responsible for the development, organization, and administration of an OPSEC program at division-level and below.. In addition to H–2, above OPSEC officers—

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

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

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

d. As required, write OPSEC documents, annexes, and appendices to OPLANs and OPORDs. Write OPSEC SOPs/plans as required for activities not covered by OPLANs and OPORDs.

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

H–5. Operations security coordinator duties

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

H–6. Qualifications for operations security program manager/officer/coordinator

a. Experience and knowledge.

(1) Operations experience is essential to the OPSEC PM, officer, and coordinator.

(2) The OPSEC PM, officer, or coordinator should have experience 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, they would have experience in the intelligence process, including intelligence analysis and estimation techniques. This experience is secondary to operations experience.

(3) Thorough comprehension of the functional relationships and procedural processes of the unit or organization.

(4) Working knowledge of Army and command planning systems, directives, and the organization's plans and procedures.

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

b. Training and education.

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

(2) OPSEC officer is required to attain Level II certification and is encouraged to attain Level III certification based on recommendation from chain of command and OPSEC program manager.

(3) OPSEC coordinator is required at a minimum to complete the IOSS OPSEC Fundamental Course (OPSE 1301) or equivalent. If executing duties as described in paragraphs H–3 or H–4, above, these individuals are now performing the duties of an OPSEC officer and will attend OPSEC Level II certification.

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

c. OPSEC skills.

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

(2) Ability to integrate and coordinate OPSEC planning with the other capabilities of IO.

d. Communicative skills.

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

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

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

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

Appendix I
Annual Operations Security Report Format

I–1. Overview of operations security program status

The annual OPSEC report is used to gather information throughout the Army on OPSEC programs. This information will be consolidated into a report to the OUSD(I) to provide a status on Army OPSEC programs. The purpose of this report is to identify Army OPSEC challenges and to chart a way ahead that feeds resourcing justifications and decisions. The OPSEC report is the Army's opportunity to shape Office of the Secretary of Defense resource decisions regarding OPSEC.

a. ACOMs, ASCCs, and DRUs will send a report to Army OPSEC PM at DCS, G–3/5/7 (G–39). Units at corps and below, activities, and installations will send a report to their respective ACOM, ASCC, or DRU. The Army OPSEC PM will send a consolidated report to the OUSD(I).

b. The reporting period is from 1 October to 30 September of the prior fiscal year. The Army OPSEC PM will specify a suspense date via ALARACT message for ACOMs, ASCCs, and DRUs to submit their reports.

I–2. Operations security report format for Army commands, Army service component commands, and direct reporting units

ACOMs, ASCCs, and DRUs will consolidate all subordinate inputs into a single report.

a. Program management. Provide a description of the command's OPSEC program management with the following details:

(1) Indicate how many full-time and part-time personnel are assigned to your OPSEC program.

(2) Have you received OPSEC assistance from, or utilized the services of, the Army OSE or the IOSS?

(a) If yes, what kind of support? (OPSEC assistance may include staff assistance, program development, planning, or training support.) If any requests were unfulfilled, please explain the circumstances.

(b) What OPSEC training has the command's OPSEC program manager received?

(3) What does your organization do to make OPSEC a priority?

b. Program plans and procedures. Summarize how well subordinate organizations are executing DOD and Army guidance on OPSEC planning and implementation with the following details:

(1) List the OPSEC policies and planning guidance your organization has issued.

(2) Have you identified the critical information within your organization?

(a) How is that critical information communicated to the command's staff and personnel?

(b) How is the CIL kept up to date as missions change?

(3) Discuss the OPSEC measures that your command employs.

(4) Have you developed procedures and/or tools to assist with OPSEC implementation? If yes, please describe, and indicate whether this could be shared with other Army elements and DOD.

(5) Describe the procedures and protocols used to review open source material for critical and sensitive information.

(6) Describe the process to include OPSEC in the review of information prior to public release.

c. Assessments. This section requests information on the command's OPSEC assessments, assessment findings and trends, and corrective actions. Please provide the following details:

(1) Did you conduct an annual OPSEC assessment? Please describe the type of assessment performed. (Assessments may include self-assessments, assessments and/or surveys supported by the IOSS or Joint OSE, or another type of program review.)

(2) Did your command request assessment assistance from outside sources? If so, from which sources and for what support?

(3) What OPSEC trends and issues were identified by your assessment(s)? (Provide a summary, without unit specific information, on trends or issues which could indicate an Army-wide OPSEC issue.)

d. OPSEC training and awareness. Provide an assessment of the command's OPSEC training and awareness programs with the following details:

(1) Describe the command's OPSEC awareness program.

(2) Have you identified OPSEC training requirements commensurate with the respective responsibilities of OPSEC assigned personnel? Please describe (for example, training requirements for OPSEC program managers, planners, OPSEC coordinators, OPSEC working group, and so forth).

e. Program resources. Summarize the command's investment in the OPSEC program with the following details:

(1) Describe what resources you apply to your OPSEC program. (Applied resources might include awareness products, conference fees, mobile training teams, and so forth)

(2) Describe funding shortfalls in the command's OPSEC program.

f. Miscellaneous problems and recommendations. Address problems, not previously addressed, that impact on the command's overall OPSEC posture. Such problems might include personnel manning or administrative problems.

g. 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 previously discussed.

h. Pre- and post deployment actions. How is OPSEC training provided in conjunction with pre- and post deployment actions per AR 530–1 and AR 350–1. If not, why not?

i. Trained personnel. How does your command ensure there are enough Level II trained personnel to meet your command's requirements?

Appendix J
Annual Army Operations Security Achievement Awards Program

J–1. Purpose

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

J–2. Scope

a. Period. These awards cover the period from 1 October through 30 September of each fiscal year.

b. Award categories.

(1) Organizational achievement award. This award is for any size unit, organization, or activity with two levels; brigade and below, and division and above or equivalent.

(2) Individual achievement award. This award recognizes outstanding U.S. Government employees; contractors are not eligible.

(3) Multimedia achievement award. This award is for all Army personnel, excluding contractors.

c. Limitation. Organizations may submit only one nominee in each of the above categories.

J–3. Awards criteria

a. Organizational achievement award. The organizational achievement award recognizes the organization that contributed the most to the advancement and practice of OPSEC in the government community for the previous fiscal year. Nominations will be judged on the following criteria:

(1) Evidence of organizational ability to identify and solve significant OPSEC problems, threats, or vulnerabilities.

(2) Creation or development of innovative programs for OPSEC training and education.

(3) Mission accomplishments and successes at the organizational level resulting from the application of OPSEC and/or development of a robust OPSEC program.

(4) Implementation of significant measures to prevent, eliminate, or reduce threats or vulnerabilities.

(5) The nomination must be in a narrative format (no bullets) and must be no more than 3 pages, single-spaced, Times New Roman font, 12 pitch, and staples must not be used. It must describe the specific accomplishments of the nominated organization, focusing solely on the OPSEC achievements. All packages not prepared in accordance with these instructions will be considered ineligible.

b. Individual achievement award. This award recognizes an outstanding U.S. Government employee's accomplishments during the preceding fiscal year. Individuals will be judged on the following criteria:

(1) Evidence of individual ability to identify and solve significant OPSEC problems, threats, or vulnerabilities.

(2) Demonstration of outstanding leadership and knowledge in the application of OPSEC.

(3) Innovative and creative use of resources (for example, personnel, fiscal, networking, or facilities) to successfully accomplish OPSEC related goals and missions.

(4) 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.

(5) An achievement that leads to an improvement in the Army or organizational OPSEC posture.

(6) Nominees should have demonstrated personal initiative in application of OPSEC policy and doctrine.

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

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

(9) 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.

(10) The nomination must be in narrative format (no bullets) and must be no more than three pages, single-spaced, Times New Roman font, 12 pitch, and staples must not be used. It must describe the specific accomplishments of the nominated individual, focusing solely on OPSEC achievements, as opposed to other, non-OPSEC security functions. All packages not prepared in accordance with these instructions will be considered ineligible.

c. Multimedia achievement award. This award is given in recognition of outstanding multimedia accomplishments by U.S. Government organizations or employees during the preceding fiscal year. These awards are designed to stimulate the development and distribution of OPSEC-related education and awareness materials. Multimedia achievement award is judged on the following criteria:

(1) Be original work created by U.S. Government organizations or employees, or include work created by U.S. Government contractors of which the U.S. Government has unlimited rights.

(2) Possess a valid OPSEC educational, training, or awareness theme or message.

(3) Demonstrate artistic value and visual impact.

(4) The nomination narrative must be no more than two pages, single-spaced, Times New Roman font, 12 pitch, and describe the product, its use (for example, training awareness, and so forth), benefits, and impact on the organization. A total of six copies (original and five copies) of the nominated material (for example, poster, publication, compact disc (CD)) shall be included in the submission package. All packages not prepared in accordance with these instructions will be considered ineligible.

(5) For poster nominations, submit one original poster mounted on foam board or equivalent no smaller than 8 1/2" x 11" and no larger than 30" x 40". The five copies must be no smaller than 8 1/2" x 11" and are not required to be mounted.

(6) All multimedia nominations must include certification that the product either contains no copyrighted or trademarked material, or includes copyrighted or trademarked material to which the U.S. Government has unlimited rights.

J–4. Submission requirements

All Department of the Army nomination packages must be submitted to the Army OSE through the award nominees ACOM, ASCC, or DRU OPSEC PM. All waivers must be approved by the Army OPSEC PM, in writing.

a. Organizational and individual submission package must contain the following:

(1) A one-page endorsement letter signed by the head of the submitting organization.

(2) A nomination narrative as required by the award criteria.

(3) A CD containing 30 to 40 digital photographs in .jpg format of the award nominees (individuals or organizations). Photos must be unclassified. "Action shots" are preferred. For winning submissions, these photos will be used in creating the awards video shown during the awards ceremony. CDs will not be returned to the submitter. The submitter

must also include a certification that the U.S. Government has an unlimited rights license (for example, copyright and trademark) to any third party intellectual property contained on the CD.

b. For multimedia achievement award submissions—

(1) Certification that the U.S. Government has an unlimited rights license to any third party intellectual property (for example, copyright and trademark) to any third party intellectual property contained with the submission.

(2) The original and five copies of the nominated product (for example, CD, poster, and so forth) as required by the award criteria.

c. Additional submission requirements—

(1) All written paperwork must be on 8 1/2" x 11" paper not bound by staples and without amplifying pictures, artwork, attachments, or cover pages.

(2) The submission narrative must address all award selection criteria.

(3) Responsibility for prepublication review of any submitted materials rests with the submitter.

d. Nominations from ACOMs, ASCCs, and DRUs are due to the Army OSE no later than 15 November for the preceding fiscal year.

J–5. Selection process

Army OPSEC PM will form a selection committee consisting of representatives from DCS, G–3/5/7 (G–39) and the Army OSE to select the organization, individual, and multimedia award winners.

J–6. Recognition

a. The committee will select winners in all categories by 1 December for the preceding fiscal year.

b. First place winners in each category will receive a congratulatory letter from the Chief of Staff, Army.

c. Second and third place winners in each category will receive a congratulatory letter from the Army OPSEC proponent, DCS, G–3/5/7.

d. First, second, and third place winners will be the Department of the Army's nominees for the National OPSEC Achievement Awards Program at the federal government level.

Appendix K
Army Commands, Army Service Component Commands, and Direct Reporting Units

K–1. Definitions

The following definitions are provided for reference only, and are derived from AR 10–87. Refer to the most recent version of AR 10–87 for the current list of ACOMs, ASCCs, and DRUs describe Army units as designated by the SA, who previously directed the realignment of Army headquarters in order to more effectively and efficiently provides support to the transformed, campaign-quality operating force with Joint and expeditionary capability.

a. Army command. An ACOM is an Army force, designated by the SA, performing multiple Army Service Title 10 functions (10 USC 3013) across multiple disciplines. Command responsibilities are those established by the Secretary.

b. Army service component command. An ASCC is an Army force, designated by the SA, comprised primarily of operational organizations serving as the Army component of a combatant command or a subunified command. If directed by the combatant commander, an ASCC serves as a Joint Forces Land Component Command, or Joint Task Force. Command responsibilities are those assigned to the combatant commanders and delegated to the ASCCs and those established by the SA.

c. Direct reporting unit. A DRU is an Army organization comprised of one or more units with institutional or operational support functions, designated by the SA, normally to provide broad general support to the Army in a single, unique discipline not otherwise available elsewhere in the Army. DRUs report directly to a HQDA principal and/or ACOM and operate under authorities established by the SA.

K–2. Unit listing

The following Army elements are designated as ACOMs, ASCCs, and DRUs:

a. ACOMs.

(1) U.S. Army Forces Command.

(2) U.S. Army Materiel Command.

(3) U.S. Army Training and Doctrine Command.

b. ASCCs.

(1) U.S. Army Africa.

(2) U.S. Army Central.

(3) U.S. Army Europe.

(4) U.S. Army North.
(5) U.S. Army Pacific.
(6) U.S. Army Space and Missile Defense Command/Army Forces Strategic Command.
(7) U.S. Army Special Operations Command.
(8) U.S. Army South.
c. DRUs.
(1) 2nd Army.
(2) Military District of Washington.
(3) U.S. Army Acquisition Support Center.
(4) U.S. Army Corps of Engineers.
(5) U.S. Army Criminal Investigation Command.
(6) U.S. Army Installation Management Command.
(7) U.S. Army Intelligence and Security Command.
(8) U.S. Army Medical Command.
(9) U.S. Army Test and Evaluation Command.
(10) U.S. Army War College.
(11) U.S. Military Academy.
d. Service component command. U.S. Army Cyber Command.
e. United States Army National Guard (54 states and territories).
f. U.S. Army Reserve.

Appendix L
Information That May Be Exempt from Release under the Freedom of Information Act

L–1. Exemptions

Only information that falls in the following categories may qualify as exempt from public disclosure under FOIA.

a. Exemption 1. Information which is currently and properly classified.

b. Exemption 2.

(1) Information which pertains solely to the internal rules and practices of the agency. On March 7, 2011, the U.S. Supreme Court issued an opinion pertaining to Exemption 2 of FOIA (5 USC 552(b).2) that overturned 30 years of established FOIA precedents and significantly narrowed the scope of that exemption. See Milner v. Dept of the Navy,131 S. Ct. 1259 (2011).

(2) Based on that text, and as set forth by the Supreme Court's decision in Milner, there are three elements that must satisfied in order for information to fit within Exemption 2.

(a) The information must be related to "personnel" rules and practices.

(b) The information must relate "solely" to those personnel rules and practices.

(c) The information must be "internal."

(3) The language provided for exemption of matters "related solely to the internal personnel rules and practices of an agency" 5 (USC 552(b)(2)). Thus, the old formulations of "High 2" and Low 2" - which were based on legislative history and not on this statutory language - no longer control. There is now just "Exemption 2" which is defined according to its text.

c. Exemption 3. Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.

d. Exemption 4. Information, such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis, which, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness.

e. Exemption 5. Intra-agency memoranda which are deliberative in nature; this exemption is appropriate for internal documents which are part of the decision making process and contain subjective evaluations, opinions and recommendations.

f. Exemption 6. The release of information which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.

g. Exemption 7. Records of information compiled for law enforcement purposes that:

(1) Could reasonably be expected to interfere with law enforcement proceedings.

(2) Would deprive a person of a right to a fair trial or impartial adjudication.

(3) Could reasonably be expected to constitute an unwarranted invasion of personal privacy of others.

(4) Disclose the identity of a confidential source.
(5) Disclose investigative techniques and procedures.
(6) Could reasonably be expected to endanger the life of physical safety of any individual.
h. Exemption 8. Certain records of agencies responsible for supervision of financial institutions.
i. Exemption 9. Geological and geophysical information concerning water and oil wells.

L–2. References
For more information on FOIA, refer to AR 25–55 and AR 380–5.

Appendix M
Format for Operations Security Annex/Appendix/Tab to Operation Plan/Operation Order

M–1. General
An OPLAN or OPORD can include OPSEC in an annex. It can also be an appendix to an annex, or a tab to an appendix to an annex.

M–2. Procedures
Figure M–1 can be used as a format to cover OPSEC in an OPLAN or OPORD. The format and contents of the five paragraphs and their subparagraphs remain the same as in an OPLAN or OPORD.

Annex or Appendix ___ (OPSEC) to XXXXX (Identify what this is an Annex or Appendix to)

1. SITUATION

a. Adversary.

(1) Identify the estimated adversary assessment of friendly operations, elements, and intentions.

(2) Identify adversary intelligence collection elements according to major categories (for example, All-Source Intelligence, HUMINT, IMINT, SIGINT, MASINT, TECHINT, and Counterintelligence).

(3) Identify potential sources (including other nations) that provide support to the adversary.

(4) Identify unofficial intelligence organizations that support the national leadership, if any.

(5) Identify the adversary intelligence element strengths and weaknesses.

b. Friendly.

(1) State the Critical Information of the higher headquarters.

(2) State the Critical Information of the command (or activity/operations).

(3) Identify the major OPSEC tasks.

c. Attachments and detachments.

(1) Identify any attachments required to conduct OPSEC.

(2) Identify any detachments of units that enhance the OPSEC posture of the command.

2. MISSION. State how OPSEC will protect the Critical Information and support the commander's objectives.

3. EXECUTION.

a. Scheme of support.

(1) OPSEC tasks. Describe as phased operations, where applicable. Describe how OPSEC will help achieve the commander's intent and endstate.

(2) List the OPSEC task not listed in the base OPLAN/OPORD/Plan to be performed by elements of the command.

(3) List the OPSEC measures to be taken by the unit to ensure collection efforts are negated or reduced to an acceptable level.

(4) List the security methods, assets and programs of special importance to the operation. Include personal security, physical security, COMSEC, SIGSEC, patrolling, counter reconnaissance, and so forth. Ensure efforts are aimed at both external and internal security threats.

(5) State how OPSEC supports traditional security discipline elements.

(6) Identify how OPSEC monitoring will be accomplished to ensure effectiveness of OPSEC measures during execution.

Figure M–1. Sample format for OPSEC annex/appendix/tab to OPORD/OPLAN

(7) Identify any OPSEC-related intelligence reports needed for feedback.

(8) Identify OPSEC after action reports (AAR) requirements.

b. Tasks to subordinate units.

(1) List OPSEC measures that specific units/elements are to implement.

(2) List the OPSEC measures that require special emphasis by assigned, attached, or supporting units/elements. These are OPSEC measures that are implemented to counter a specific adversary collection threat. List these by phase, and identify specific responsibilities for subordinate elements/units.

c. Coordinating instructions.

(1) Identify OPSEC measures common to two or more elements/units.

(2) Identify the required coordination with the public affairs office (PAO)

(3) Identify OPSEC measure termination by measure.

(4) Identify guidance for---

(a) Declassification of information.

(b) Public release of OPSEC-related information.

4. SERVICE SUPPORT. Identify, if any, the OPSEC-related supply support requirements.

5. COMMAND AND SIGNAL

a. Command. State the location of the OPSEC officer/office.

b. Signal. State any special or unusual OPSEC-related or OPSEC specific communications, reporting, or notification requirements, if any.

Figure M–1. Sample format for OPSEC annex/appendix/tab to OPORD/OPLAN–continued

Appendix N
Format for Operations Security Documents

N–1. General
An OPSEC plan/SOP should include sensitive mission areas and critical information, the intelligence collection threat, concept of implementation, and taskings/responsibilities. An OPSEC estimate can be added as an appendix and should include critical information/essential elements of information, indicators, and adversary threat.

N–2. Procedures
Figures N–1, N–2, and N–3 can serve as a guide when writing an OPSEC plan for activities, programs, or projects not documented by an OPORD or OPLAN. This model applies to RDT&E Programs, Contract Programs, the Acquisition Systems Protection Program and SAPs.

(CLASSIFICATION)

HEADQUARTERS
UNITED STATES ARMY XXX XXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX 123454789

SUBJECT: Operations Security (OPSEC) Plan for XXXXX

1. ( ) References:

a. AR 530-1, OPSEC

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 critical information.

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, stares, transmits, or transfers information or data (including weapons systems related technology, or system critical program information (CPI) that is classified or falls within the definition of unclassified sensitive and/or critical information. Every effort should be made to keep OPSEC plans and the critical information list (CIL) unclassified. Classified portions, such as threat information, should be published and provided as separate appendixes.

(3) ( ) An area of activity or experimentation, 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. ( ) Critical information. State the current critical information that applies to all elements of the organization, activity, or program on a continuous basis, or for a specified duration of time. The specific critical information for a particular element group, action, or activity, should be published in appendix 1, OPSEC Estimate, at paragraph 1, Critical information. (See app 1, Sample OPSEC Estimate.)

4. ( ) The intelligence collection threat.

Figure N–1. OPSEC plan

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 4h of app 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 counter analysis). Refer to appendix 2, OPSEC Measures for detailed planning guidance.

5. ( ) Concept of implementation. State the commander's intent for 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 or visits by foreign personnel.) 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, OPSEC Measures.

NAME
General, USA
Commanding

Appendices
1. OPSEC Estimate
2. OPSEC Measures

Official;

/S/

NAME
Deputy Chief of Staff, Operations

CLASSIFIED BY:
DECLASSIFY:

(CLASSIFICATION)

Figure N–1. OPSEC plan—continued

(CLASSIFICATION)

Appendix 1 (OPSEC Estimate) to OPSEC Plan for XXXXX XXXX

1. ( ) Critical information.

a. ( ) State the critical information. Critical information consists of "specific facts about friendly intentions, capabilities, limitations, vulnerabilities, and activities vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment. Non-tactical organizations (such as RDT&E activities test and evaluation activities, weapons systems test ranges, and technology development activities) state critical information in the same manner as tactical units. The critical information may be for an activity, phase of an operation, specific function, or other logical group.

Examples (For additional examples, see app C of AR 530-1)---

(1) ( ) The maximum range of the M-213B Controlled Fragmentation Projectile, when fired from the improved MK19 Weapons System.

(2) ( ) The dates for the Ground Launched Short Range Anti-Radiation Attack Missile test.

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

(4) ( ) Type discrimination logic imbedded in the M57A1 IR Homing Sensor, used with the MK65 LGB.

b. ( ) The CIL may be a tab to this appendix or a separate document. This may be desirable when the organization will provide the CIL 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 CIL. State whether classified or unclassified.

3. ( ) Detectable activities (For additional example, see app D of AR 530-1). Identify the activities that are or will be detectable during the conduct of the activity, action, or function. These are OPSEC indicators. List the indicators by type in this paragraph, or attach as a tab to this appendix. See appendix D 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.

Figure N–2. Appendix 1 to OPSEC plan

(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.

(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) ( ) Identity 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, identity 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 newspapers.

(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 over flight 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 (4000M) SE, ground, day/night imagery.

(3) ( ) SIGINT collection (pre-test, test, post test).

Figure N–2. Appendix 1 to OPSEC plan—continued

(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) ( ) Coven sensors implanted adjacent to range facility.

(b) ( ) Coven 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)

Figure N–2. Appendix 1 to OPSEC plan—continued

(CLASSIFICATION)

Appendix 2 (OPSEC Measures) to Operations Security Plan for XX XXX 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 and SIGINT).

(b) ( ) Open source program documentation (HUMINT).

(c) ( ) Unsecured telephone (SIGINT).

(d) ( ) Public domain briefing/presentations (HUMINT).

(e) ( ) Foreign travel (HUMINT and SIGINT).

(2)( ) Contractor facility vulnerabilities.

(a) ( ) Unsecured AIS systems, to include small computer systems (HUMINT and SIGINT).

(b) ( ) Open source program documentation (HUMINT).

(c) ( ) Corporate public affairs releases and marketing.

(d) ( ) Unsecured telephone/FAX, contractor to subcontractor (SIGINT).

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

b. ( ) OPSEC measures. Identify the measures 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 per CIO/G-6 SOP; all personnel assigned to PM office will receive an information system security (1SS) briefing prior to operating a PM office AIS.

Figure N–3. Appendix 2 to OPSEC plan

(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 any foreign travel.

(e) ( ) All information concerning XXXXX XXXXX program shall be reviewed, according to the CIL, prior to any public release.

(f) ( ) All personnel assigned to or supporting/having contact with XXXX 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.

(2)( ) OPSEC measures.

(a) ( ) The PM office security officer will coordinate with supporting intelligence CI personnel for FBI and CI counter-espionage briefings and matters.

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

(3) ( ) Counter analysis.

(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 N–3. Appendix 2 to OPSEC plan—continued

Appendix O
Internal Control Evaluation

O–1. Function
The function covered by this evaluation is the implementation of Army OPSEC policy as outlined in this regulation.

O–2. Purpose
The purpose of this evaluation is to assist commanders at all levels in evaluating the following key internal controls contained in this regulation. It is not to cover all controls.

O–3. Instructions
These key controls must be formally evaluated at least once every 5 years or whenever internal controls administration changes. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification). Evaluation test questions are outlined in paragraph O–4, below and are intended as a start point for each applicable level of internal control. Answers must be based on actual testing of key internal

controls. Answers that include deficiencies must be explained and the corrective action indicated in supporting documentation.

O–4. Test questions

a. Establishment of OPSEC education and training.

(1) Has the DCS, G–3/5/7, through Commander, TRADOC, coordinated with Army training institutions to integrate OPSEC fully into curricula throughout officer, warrant officer, NCO and civilian education systems?

(2) Has the DCS, G–3/5/7, in coordination with Commander, 1st Information Operations Command (Land), completed an annual report describing the Army's progress in meeting DOD requirements for a trained OPSEC cadre with the DA Career Force.

(3) Has the Commander, 1st IO CMD(L) developed and is the 1st IO CMD(L) teaching the Army's HQDA PMs and OPSEC Officers course in sufficient iterations and quotas to train the force?

b. Implementation of responsibilities under this regulation.

(1) Has the DCS, G–3/5/7 developed OPSEC policies that are consistent with DOD and Joint policies, guidance and instructions?

(2) Have ACOMs, ASCCs, and DRUs appointed a non-contractor staff position to become the command's OPSEC PM?

(3) Is the Army OPSEC PM maintaining an archive of ACOMs, ASCCs, DRUs annual OPSEC reports that include Program Management, Program Plans and Procedures, assessments, and OPSEC Training and Awareness?

(4) Has the Army OPSEC PM established, chaired and managed an OPSEC Working Group comprised of ACOMs, ASCCs, and DRUs OPSEC PMs?

c. Development of OPSEC capability in the Army.

(1) Do personnel assigned to OPSEC PM/OPSEC Officer positions meet the eligibility criteria outlined in Appendix H?

(2) Does the DCS, G–3/5/7, in coordination with the 1st IO CMD(L), maintain an OPSEC-trained personnel database to track OPSEC-trained personnel across the Army?

(3) Are Doctrine, Organization, Training, Material, Leadership and education, Personnel, Facilities solutions being applied to OPSEC shortfalls or problem sets identified by ACOMs, ASCCs, and DRUs?

Glossary

Section I
Abbreviations

ACOM
Army command

AIS
Automated Information System

ALARACT
All Army activities

AMC
Army Materiel Command

ASCC
Army service component command

ATEC
Army Test and Evaluation Command

AWRAC
Army Web risk assessment cell

Blog
Web log

CD
compact disc

CFR
Code of Federal Regulations

CI
counterintelligence

CIL
critical information list

CIP
command inspection program

CJCSI
Chairman, Joint Chiefs of Staff Instruction

COA
course of action

COMINT
communications intelligence

COMSEC
communications security

CPI
critical program information

CUI
controlled unclassified information

DA
Department of the Army

DCI
Defense Critical Infrastructure

DCIP
Defense Critical Infrastructure Program

DCS
Deputy Chief of Staff

DEA
Drug Enforcement Administration

DOD
Department of Defense

DODD
Department of Defense Directive

DODI
Department of Defense Instruction

DODM
Department of Defense Manual

DRU
direct reporting unit

EAR
Export Administration Regulations

ELINT
electronic intelligence

ELSEC
electronic security

EO
executive order

EOP
external official presence

FISINT
foreign instrumentation signals intelligence

FM
field manual

FOIA
Freedom of Information Act

FOUO
for official use only

FRG
Family Readiness Group

FRSA
Family Readiness Support Assistant

HQDA
Headquarters, Department of the Army

HUMINT
human intelligence

IA
Information Assurance

IMINT
imagery intelligence

INFOSEC
information security

IO
information operations

IOSS
interagency operational security support staff

ISR
Intelligence, surveillance and reconnaissance

ITAR
International Traffic in Arms Regulations

JCS
Joint Chiefs of Staff

MASINT
measurement and signatures intelligence

MILDEC
military deception

NCO
noncommissioned officer

NSDD
National Security Decision Directive

OIP
organizational inspection program

OPLAN
operation plan

OPORD
operation order

OPSEC
operations security

OSE
Operations Security Support Element

OSINT
open-source intelligence

OUSD(I)
Office of the Under Secretary of Defense (Intelligence)

PAO
public affairs officer

PEO
program executive officer

PM
program manager

POI
program of instruction

PPP
program protection plan

PWS
performance work statement

RA
requiring activity

RDT&E
research, development, test, and evaluation

SA
Secretary of the Army

SAP
Special Access Program

SIGINT
signals intelligence

SOF
special operations forces

SOO
statement of objectives

SOP
standard operating procedure

SOW
statement of work

TECHINT
technical intelligence

TRADOC
Training and Doctrine Command

UCMJ
Uniform Code of Military Justice

UCNI
Unclassified Controlled Nuclear Information

USC
United States Code

Section II
Terms

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

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

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

Communications security (COMSEC)
A component of IA that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material.

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

Contracting activity
An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

Contracting office
An office that awards or executes a contract for supplies or services and performs post award functions not assigned to a contract administration office.

Controlled unclassified information (CUI)
Unclassified information to which access or distribution limitations have been applied according to national laws, policies, and regulations of the U.S. Government. It includes U.S. information that is determined to be exempt from public disclosure according to DODD 5230.25, DODD 5400.07, AR 25–55, AR 340–21, AR 530–1, and so on, or that is subject to export controls according to the ITAR or the EAR.

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

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

Critical information
Information important to the successful achievement of U.S. objectives and missions, or which may be of use to an adversary of the United States. Critical information consists of specific facts about friendly capabilities, activities, limitations (includes vulnerabilities), and intentions needed by adversaries for them to plan and act effectively so as to

degrade friendly mission accomplishment. Critical information is information that is vital to a mission that if an adversary obtains it, correctly analyzes it, and acts upon it will prevent or seriously degrade mission success. Critical information can be classified information or unclassified information. Critical information can also be an action that provides an indicator of value to an adversary and places a friendly activity or operation at risk.

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

Critical Program Information
Elements or components of an Research, Development, and Acquisitions program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. See DODI 5200.39 for more information.

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

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

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

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

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

For official use only
A designation that is applied to unclassified information that may be exempt from mandatory release to the public under FOIA.

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

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

Government contracting agency
An element of a federal department or agency that is designated by the agency head and is delegated broad authority regarding acquisition functions.

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

Information assurance
Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information operations
The employment of the core capabilities of electronic warfare, computer network operations, military information support operations, MILDEC, and OPSEC, in concert with specified and related capabilities, to affect or defend information and information systems, and to influence decision-making.

Information security
The system of policies, procedures, and requirements established under the authority of EO 12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

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

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

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

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

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

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

Military information support operations
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 military information support operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

Multidiscipline counterintelligence analysis
The process of determining the presence and nature of the total all-source adversary intelligence threat to a given 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
A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to-Identify those actions that can be observed by adversary intelligence systems.Determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Operations security compromise
The disclosure of critical information or sensitive information which has been identified by the command and any

higher headquarters that jeopardizes the unit's ability to execute its mission or to adequately protect its personnel and/or equipment.

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

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. This also forms the contents of an OPSEC estimate.

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.

Publicly accessible Web site
An Army website with access unrestricted by password or Public Key Infrastructure user authorization. "Public" refers to the at-large audience on the Internet; anyone who can access a website through a browser. (AR 25–1)

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

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

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

Sensitive activities
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 compartmented information
Information or material requiring special controls for restricted handling within compartmented intelligence systems and for which compartmentalization is essential. sensitive compartmented information rules are established by the Director of Central Intelligence.

Sources of data
Materials, conversations and actions that provide information and indicators. The sources are as follows: 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. Open sources. Oral, documentary, pictorial, and physical materials accessible to the public. 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
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 term referring to technical investigations for compromising emanations from electrically operated information processing equipment; these investigations were conducted in support of emanations and emissions security.

Threat
Capability of a potential adversary to limit or negate mission accomplishment or to neutralize or reduce the effectiveness of a current or projected organization or material item. Two types of threat information are required: Intelligence collection threat (efforts by adversary to gain information). Combat capability threat (adversary forces' weapons systems which the U.S. Army will face on the battlefield).

Section III
Special Abbreviations and Terms
This section contains no entries.