DEPARTMENT OF THE AIR FORCE
Headquarters US Air Force
Washington DC 20330-5000

AF PAMPHLET 55-36

9 July 1985

Operations

USAF OPSEC GUIDE

This is a nondirective, informational publication that shows how to apply Operations Security (OPSEC) as required by AFR 55-30, Operations Security. An effective OPSEC program can be achieved by following the guidelines it sets forth. This pamphlet provides OPSEC information for all military and civilian personnel within the US Air Force. Major commands (MAJCOM), separate operating agencies (SOA), and direct reporting units (DRU) may also use it as one of the basic OPSEC reference documents to aid in developing OPSEC programs. MAJCOMs, SOAs, and DRUs should consider the need for additional manpower as they implement their OPSEC program at lower echelons. Send recommended changes through channels to HQ USAF/XOEO, Wash DC 20330, with an information copy to Headquarters Electronic Security Command (HQ ESC/DOOO), San Antonio TX 78243.

No. of Printed Pages: 16
OPR: XOEO (Capt David McNamee)
Approved by: Col Richard P. Wallace
Writer-Editor: R. M. Downey
Distribution: F

Section A—Administration

1. Purpose. This pamphlet gives OPSEC officers a basis on which they can build an effective OPSEC program. The contents have been, in part, compiled from various DOD sources. The authors have attempted to cover all phases of the OPSEC program, from initial orientation to conducting an OPSEC survey. *The pamphlet is general by design.* OPSEC officers are encouraged to add to this pamphlet to fit their command needs.

2. Definition. Operations Security (OPSEC) is the process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities (AFR 55-30). OPSEC applies to all levels and should be emphasized from the highest echelon down to the lowest shop and office level within a command. Essentially, OPSEC has two objectives: protecting friendly operations and degrading an adversary's war fighting capabilities through denial of critical information necessary for planning and decision making.

3. Responsibilities:

a. General Responsibilities. OPSEC policy, concepts, and standards are provided in JCS Publication 18. AFR 55-30 establishes the Air Force OPSEC program. The office of primary responsibility (OPR) for OPSEC at HQ USAF is the Deputy Chief of Staff, Plans and Operations, through the Directorate of Electronic Combat (HQ USAF/XOE). Each MAJCOM has a full-time OPSEC officer. SOAs and DRUs have either a full-time OPSEC officer or a designated OPSEC OPR.

b. Commanders' Responsibilities. Commanders have overall responsibility for OPSEC within their command. They are responsible for developing and implementing policy, instructions, and training necessary to maintain an effective unit OPSEC program. Specific responsibilities include:

(1) Defining which elements of the unit mission are considered critical, the compromise of which could jeopardize the unit's capability to perform its mission.

(2) Identifying those sensitive mission areas requiring protection from public exposure or hostile exploitation.

(3) Taking protective measures necessary to prevent disclosure of sensitive information.

(4) Establishing and maintaining an OPSEC education program to increase, at all levels of command, knowledge of the dangers from enemy foreknowledge of friendly operations.

(5) Assessing the unit's OPSEC posture.

(6) Establishing an OPSEC board or working group as required.

(7) Submitting an annual OPSEC report (see attachment 1).

c. OPSEC Officers' Responsibilities. OPSEC officers act as the commander's authority for implementing and maintaining the unit OPSEC program. For operational units, it is recommended that an OPSEC point of contact (POC) be designated at wing level or equivalent to manage the overall program and documentation. At subordinate units, it is recommended that a POC be designated for unit OPSEC application day-to-day airborne tactics and planning vice OPSEC program management and documentation. OPSEC Officers are responsible for:

(1) Ensuring the OPSEC has been included in all unit plans, operations orders (OPORD), operation plans (OPLAN), exercises, and daily operational activities.

(2) Ensuring that essential elements of friendly information (EEFI) are properly developed, ranked by priority, and kept current.

(3) Assembling, evaluating, and disseminating threat information.

(4) Evaluating previously identified OSPEC weaknesses in light of current threat information or exploitable conditions to determine vulnerability.

(5) Making recommendations to the commander for correcting noted deficiencies.

(6) Preparing, maintaining, and presenting OPSEC educational material to all unit personnel.

(7) Ensuring that OPSEC board agendas are prepared and board minutes are distributed.

d. Individual Responsibilities. Individuals are responsible for complying with established security practices for protecting classified, unclassified, and sensitive information which they have been exposed to. All personnel should:

(1) Be aware of the threat.

(2) Know local EEFI.

(3) Ensure co-workers are aware of threats and EEFI.

(4) Know where to obtain OPSEC guidance, such as regulations and pamphlets.

4. Organizing:

a. Regulations and OPSEC Officer Guides:

(1) The OPSEC officer should be thoroughly familiar with the various regulations and guides which define OPSEC policy and concepts and

should have copies available as reference material. These documents may be ordered through normal unit PDO channels.

(2) The regulations and guides that each OPSEC officer should have are:

(a) JCS Publication 18, Operations Security.

(b) AFR 55-30, Operations Security.

(c) Command supplement to AFR 55-30 (if published).

(d) Unit supplement as applicable.

(e) JCS OPSEC Survey Planning Guide (J3M-947-83).

(f) Air Force OPSEC Pamphlet.

(g) *The Intelligence Threat: A Handbook for OPSEC Officers*, AFOSI, December 1982 (obtained through local AFOSI detachments).

(h) MAJCOM OPSEC Guide or Handbook as applicable.

(i) JCS Joint Operational Planning System (JOPS), Volume I and II, Annex L.

(j) AFR 50-1, Ancillary Training Program.

(k) AFR 28-3, USAF Operation Planning Process.

b. OPSEC File. The OPSEC file is the reference for the current status of the unit OPSEC program and future actions. The OPSEC file should be used as the basis for compiling the unit annual OPSEC report. The file should contain the following information:

(1) List of OPSEC briefings, films, video tapes, and visual aids on hand, dates given, and to whom.

(2) Recurring OPSEC threat information (for example, weekly OPSEC threat highlights).

(3) Requested OPSEC threat information (see AFR 55-30).

(4) Names of points-of-contact (POC) and telephone numbers. This list should include, but is not limited to:

(a) Parent and host organization and higher headquarters OPSEC officers.

(b) Subordinate or lateral OPSEC officer.

(c) Local AFOSI representative.

(d) Tactical deception officers.

(e) Unit planners.

(f) DCS intelligence (IN) POC.

(g) OPSEC board working group members.

(h) Other unit security program managers (for example, automatic data processing ((ADP)) information security).

(5) Unit OPSEC board or working group minutes.

(6) Master copies of OPSEC education packages distributed for reading.

(7) Documentation of educational materials provided.

(8) EEFI lists.

(9) Management Effectiveness Inspection (MEI), Operational Readiness Inspection (ORI), or Inspector General (IG) inspection items pertaining to the unit OPSEC function, including inspection reports from other units, and corrective actions taken.

(10) OPSEC survey reports.

(11) Future plans.

(12) List of documents (such as plans, OPORDS, and concepts of operations) reviewed for OPSEC consideration, date last reviewed, and next review date.

(13) Lessons learned.

(14) Copies of correspondence and reference material.

(15) Annual OPSEC report (suggest 2-year retention for trend analysis).

NOTE: The above list is not meant to be all inclusive. For quick reference, some commanders or units use a continuity folder which contains some of the above information.

c. Visibility. To be effective, an OPSEC officer should be known throughout the unit. Persons having questions concerning OPSEC should know whom to contact. The OPSEC officer should visit working sections frequently to keep abreast of changes which may affect the OPSEC posture of the unit and determine the OPSEC awareness level of individuals through personal contact. These visits afford some degree of visibility. Additionally, posters should be displayed throughout the unit identifying the OPSEC officer and how to contact him or her.

d. OPSEC Board and Working Group. These are the two bodies that combine the power to implement OPSEC at the working level.

(1) *Purpose of the OPSEC Board.* The board assists in developing OPSEC policy and in managing supporting OPSEC programs. The OPSEC board provides a forum for addressing OPSEC matters and for sending recommendations to the commander.

(2) *OPSEC Board Responsibilities.* The OPSEC board:

(a) Reviews, coordinates, and recommends OPSEC policy and programs.

(b) Reviews, coordinates, and recommends OPSEC objectives.

(c) Reviews OPSEC posture and recommends changes to programs.

(d) Recommends subjects for OPSEC surveys and survey team composition.

(e) Assigns tasks to OPSEC board members and the OPSEC working group to make sure activities are completed.

(3) *OPSEC Board Meeting.* The OPSEC board meets at the direction of the chair. OPSEC Board members may request the chair to convene special meetings as needed.

(4) *OPSEC Board Composition:*

(a) The commander or a designated representative serves as the OPSEC board chair. The OPSEC officer serves as the OPSEC advisor to the board.

(b) Each deputy commander or organizational equivalent should be a board member; small units should assign the next level of command below the commander by functional area.

(c) Functional area managers should designate one primary and one alternate member to the OPSEC board.

1. They should provide in writing, to the OPSEC officer, the names of primary and alternate representatives, and their replacements when changes occur.

2. Alternates may attend board meetings with primary representatives. Advisors may attend at the invitation of the representative, provided suitable notice is given to the OPSEC officer.

3. Offices not permanently represented on the OPSEC board may send representatives to discuss specific issues, either at the request of, or by request to, the board chair.

(5) *The Chair's Responsibilities.* The chair:

(a) If not the commander, reports to the commander on OPSEC board actions and recommendations.

(b) Schedules and presides over OPSEC board meetings.

(c) Requests briefings on specific matters of OPSEC concern from the proper organization or agency.

(d) Establishes working groups and subcommittees, when necessary, to meet OPSEC board responsibilities.

(6) *OPSEC Working Group.* The OPSEC working group, composed of action-officer-level POCs from organizations represented on the OPSEC board, supports the activities of the OPSEC board.

(a) The OPSEC officer serves as the Chair of the OPSEC Working group.

(b) The composition of the OPSEC working group may vary (depending on specific OPSEC matters under consideration). A grade or rank limitation should not be imposed on the membership in this group.

(c) OPSEC working group functions include, but are not limited to:

1. Performing tasks as assigned by the OPSEC board.

2. Developing, recommending, and coordinating agenda items for the OPSEC board chair's approval.

3. Reviewing and coordinating on OPSEC program directives and initiatives.

(d) The OPSEC working group meets at the call of the board chair or the OPSEC officer.

5. Education:

a. For operations security to be effective, all personnel should understand the concept of OPSEC and apply that knowledge and awareness when performing assigned tasks. OPSEC training programs, to be meaningful over the long term, should be related to the jobs assigned. Case studies and lessons learned should be used to illustrate OPSEC objectives and requirements. The content of material presented should be selected to answer three primary questions the audience is likely to ask:

(1) Why is OPSEC important to my organization?

(2) Why is OPSEC important to me?

(3) How can I contribute to OPSEC?

b. OPSEC educational materials are developed from many sources. All service components produce training aids that are generic to their service; all stress the need for OPSEC awareness. In the Air Force, HQ ESC provides OPSEC training materials. Individual OPSEC officers should augment materials with their own unique ideas specific to their organization. They may also send recommendations through channels to HQ ESC/DOOO, San Antonio TX 78243, for possible Air Force-wide dissemination.

c. OPSEC training materials should receive the widest distribution. To accomplish this, the OPSEC officer should set up procedures to ensure that copies of training aids received are available to unit personnel. OPSEC officers should ensure that higher headquarters know their needs. A feedback system (IG, staff assistance visits, and annual unit status reports) ensures that materials are being properly used.

d. The following are sources of educational materials:

(1) *Briefings and Films.* Briefings from HQ ESC sources are sent to the MAJCOM OPSEC OFFICER. Films are ordered through normal

audio visual channels.

(2) *OPSEC Updates*. Prepared by HQ ESC, these packages contain threat information, samples of briefings, and open source articles that emphasize different security disciplines. They are distributed several times a year to command OPSEC officers. Reproduction is authorized.

(3) *Posters*. Ideas are developed by HQ ESC or reproduced from other sources. Posters can be ordered through Air Force PDO channels.

e. According to AFR 55-30, the following training should be accomplished:

(1) Initial OPSEC awareness training.

(2) Sustained OPSEC awareness training.

(3) Specialized training for operations planning.

f. Annual training reports are submitted according to AFR 50-1.

Section B—Relationships

6. Relationship to Other Security Programs. OPSEC encompasses aspects of other security programs. However, it should not be regarded as a managing tool for those programs; rather it integrates their effects and identifies disclosure problem. It focuses on all means of information flow and disclosure, whether or not it falls under a designated security program.

7. Relationship to Planners:

a. OPSEC officers at all levels of command should ensure that OPSEC measures are considered during the planning process.

b. Under AFR 55-30, OPSEC officers are to assist planners in identifying EEFI, associated OPSEC indicators, and protective measures for inclusion in any military activity, function, or event that requires the protection of information to deny a potential enemy either a tactical or strategic advantage.

c. OPSEC officers should become familiar with the planning process. AFR 28-3, USAF Operation Planning Process, Annex L, Appendices 1 and 2, specify those steps necessary to drafting an OPSEC annex to plans.

d. The OPSEC officer should encourage planners to develop new concepts, procedures, actions, and OPSEC initiatives to overcome OPSEC vulnerabilities. Planners should be educated to understand the importance of OPSEC. Planners should take a new look at OPSEC and understand that OPSEC needs to be included in all aspects of the plan from its inception and continually evaluated until the activity is completed.

8. Relationship to Tactical Deception Officer (TDO):

a. OPSEC officers and TDOs, when assigned, should establish a close working relationship to ensure that commanders are afforded the full range of coordinated OPSEC and deception to support operational planning.

b. Tactical deception can be defined as those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. In contrast, OPSEC is oriented towards suppressing or denying the real indicators to the enemy. The two programs are, therefore, complementary and OPSEC should be applied to all phases of the deception planning process.

c. OPSEC officers will find it beneficial to enlist the assistance of a TDO when correcting a weakness or hiding indicators of an impending operation or activity. The TDO may be able to devise a tactical deception scheme to cover the weakness or manipulate indicators so as to show something other than the real operation. The use of tactical deception should be considered early in the OPSEC planning process in order to gain full benefit.

Section C—The OPSEC Process

9. Introduction. OPSEC is a continuous, systematic process encompassing security and common sense. It can be applied to any program, plan, or operation. The basic steps are:

a. Identifying the operation or activity.
b. Determining EEFI.
c. Identifying hostile intelligence threat.
d. Assessing vulnerabilities.
e. Developing and using protective measures.
f. Evaluating protective measures.
g. Analyzing risk and commander's decisions.
h. Executing and monitoring operation.
i. Receiving feedback (lessons learned).

NOTE: This section provides guidance for the application of this process. When all steps are completed, the unit commander should be better able to evaluate the level of security provided and what EEFI information might compromised.

10. Operation or Activity. Determining the objectives of a planned operation or activity to include both operational and support mission requirements.

11. Essential Elements of Friendly Information (EEFI):

a. EEFI are critical facts about friendly operations and activities which, individually or in the aggregate, reveal sensitive details about capabilities or intentions and thus require protection from hostile intelligence collection and exploitation.

(1) EEFI parallel the key questions about friendly operations, capabilities, intentions, or activities likely to be asked by an opposing decision maker (the adversary's essential elements of information (EEI)) in competitive situations. Accurate EEFI identify those aspects which are critical to successful completion of the mission.

(2) EEFI should not be broad and generic but should specifically identify those critical functions which, if revealed, would impair or deny mission success. As an example of what is meant by broad, generic EEFI, assume that a Strategic Air Command (SAC) unit has established "Information Concerning Excercise" as an EEFI. SAC annually exercises the strategic force to test conventional warfare capabilities in exercise GIANT DRAGON. Public announcements of GIANT DRAGON are made 30 to 90 days before the exercise dates. An EEFI states information concerning the SAC exercise is an element that needs to be protected. The EEFI is obviously not valid as written since its protection directly conflicts with public affairs exercise objectives. A more accurate EEFI might be: "dates of exercise GIANT DRAGON before official public release."

(3) The OPSEC officer should be thoroughly familiar with the unit's peacetime and wartime mission. Without a complete understanding of what critical functions the unit is expected to do during various periods of readiness, the identification and construction of EEFI and their protection is extremely difficult.

b. Missions statements (both classified and unclassified), OPLANS, contingency plans (CONPLANS), and other planning documents tasking the unit should be reviewed. The OPSEC officer probably will find it very beneficial to organize critical unit mission functions under various major headings; for example, peacetime and wartime. Once this is accomplished, an analysis of these tasks should result in a determination of responsible or contributing functional areas (such as maintenance, logistics, operations, and administrative support). The OPSEC officer should not hesitate to contact commanders and functional area managers or the OPSEC working group to determine the extent of involvement in a particular mission phase to establish security objectives and begin developing EEFI. The function of EEFI are to describe *what* information needs to be protected, and *how long* it needs protection.

c. The OPSEC officer then presents a preliminary analysis of critical mission functions to the OPSEC board or working group. The OPSEC board or working group reviews the analysis and presents a final analysis to the commander. Following the commander's approval, the board or working group directs the construction of EEFI by functional area.

d. Each command, unit, or organization is unique and, when preparing plans, should include only those EEFI applying to its operations and activities. Subordinate units should refine EEFI listed in higher headquarters plans and orders and establish additional EEFI pertinent to their supporting plans.

e. OPSEC offices should provide guidance such as *why* certain information requires protection and *who* is most directly responsible for protecting the information. EEFI should be written into a plan as applicable. EEFI are classified according to the operation they protect and may be classified either as a whole or individually.

f. The success of an organization's OPSEC program essentially rests on developing accurate EEFI, using analysis similar to that previously mentioned; proper OPSEC planning and employment; and the education and awareness program directed at unit members. The more specific and understandable the EEFI, the easier they are to learn and protect. The commander should direct principal unit functional areas to identify elements critical to mission success.

g. To further illustrate the concept, a functional EEFI listing pertaining to security might be as follows:

(1) Specific access controls and requirements.

(2) Access lists and specific security measures.

(3) Details of the physical security system.

(4) Number of alert-team members available.

(5) Actual response time.

(6) Details of the intrusion and duress response plans.

(7) TEMPEST control and test results.

(8) Computer access passwords and phone numbers.

(9) Deficiencies and weakness of items (1) through (8) above.

h. Similar lists for all functional areas addressed to specific plans create the basis for unit OPSEC education and awareness and create a functional guideline for individual unit members.

The OPSEC program in its simplest form answers these questions:

(1) What are the questions that the enemy might ask about us? (What is sensitive?)

(2) How susceptible is the information to intelligence collection? (How is the sensitive information revealed?)

(3) How interested is the enemy, and how capable are they at collecting the information? (What is the threat?)

(4) Can we eliminate the sources of information; and, if not, how can we protect them? (Protective measures)

(5) If we can't eliminate or protect the sources of information (the intelligence indicators), how can we confuse the enemy's understanding? (Deception)

i. EEFI need not address plans and programs but could be written to protect information concerning any areas in which an adversary could identify an exploitable condition or weakness in capabilities, such as:

(1) Status of training, combat readiness, or combat efficiency of units and forces.

(2) Organizational identities, locations, movements, and strengths of specialized units or activities.

(3) Command structure changes that could reveal fundamental changes in mission or capability.

(4) Mission changes that indicate strategy or intentions.

(5) Alteration of an organization's operating capabilities.

(6) Introduction of new equipment or upgrade of current equipment.

(7) Equipment shortages or maintenance trends indicating impaired operating efficiency or combat readiness.

(8) Security clearances or special access authorizations of individuals related to special projects (observation of an individual's movements could reveal classified locations).

(9) Unique personnel, training, or organizational requirements relating to operational intent or activity.

(10) Movements of senior personnel.

(11) Maps and mapping requirements indicating planned activities or operations.

(12) Nickname of projects, operations, or activities.

NOTE: This list is not meant to be all inclusive or applicable to each organization. It provides a sample of subjects normally not considered classified, but critical to the activity.

12. Intelligence Principles. The principles of intelligence govern what information adversaries collect and how they use it. To deny, confuse, or discredit adversary intelligence, we should be familiar with intelligence principles.

a. Intelligence perform four basic missions: detection, recognition, identification, and location.

(1) Detection raises the enemy's awareness of an on-going activity. By conducting broad searches of data looking for anything peculiar, unusual, or different, they attempt to detect activity.

(2) Recognizing intentions evolves from detecting activity. Actual intentions may remain unknown, but decision makers are appraised of options they might consider, allowing them to prepare counter actions.

(3) Identification, the third mission, identifies what forces, style (tactics and procedures), and technology are to be used.

(4) Location identifies when and where something will happen.

b. Time is a critical factor in intelligence and security. If we deny adversaries intelligence indicators long enough, they may not be able to establish the truth or make a critical decision in time.

c. The value of intelligence information depends on its accuracy, timeliness, and reliability. Intelligence is a product of collection, integration, evaluation, and analysis. Raw data may have insignificant value until the intelligence process is completed.

13. Secrecy and Surprise. OPSEC is concerned with preserving secrecy and achieving surprise. Surprise is basic to all successful military operations, both defensive and offensive, and can be the most vital element for success in modern war. So obvious are the advantages of secrecy and surprise that they are the instinctive tools of survival in nature, by both the hunter and the hunted. In war, surprise has provided an overwhelming advantage by affecting the enemy's will, causing them to become confused, disconcerted, and paralyzed. Secrecy's ultimate aim is providing an advantage in combat. Offensively, secrecy and surprise aim to devastate the enemy's ability and will to resist. Defensively, secrecy prevents the enemy from knowing where or when to act, what forces to use, and what actions to take.

14. Threat:

a. A detailed explanation of the multidiscipline hostile intelligence threat to US military operations is contained in the Air Force Office of Spe-

cial Investigation (AFOSI) Special Report, The Intelligence Threat: A Handbook for OPSEC Officers, dated December 1982. The multidiscipline threat OPSEC is concerned with is posed by human intelligence (HUMINT), imagery intelligence (IMINT), and signals intelligence (SIGINT).

b. To be effective, an OPSEC program should be based on the most current intelligence threat analysis available. Local AFOSI representatives and intelligence personnel should be consulted for the threat information you need. Special threat analysis services are available from various agencies as listed in AFR 55-30. The intelligence threat should be geared to a specific operation or activity. The intelligence threat should be considered in every aspect of the OPSEC process.

c. Personnel participating in exercises or performing extended temporary duty (TDY) need to be aware of the multidiscipline threat for the area of deployment or employment. Exercise planners should add intelligence threat analysis into the planning process. They should ensure that all participating units receive copies of current threat information. Arrangements should be made for either the host base to provide exercise participants with a current threat briefing before they depart their home station or personnel should be briefed upon arrival. In either case, host base intelligence and/or counterintelligence activities should be contacted on arrival for updated local-area threat information.

d. If your unit makes frequent deployments, current threat information should be available for all deployment locations and all personnel should be briefed before departure. EEFI and protective measures should be identified for deployed locations as the threat for the deployed location may differ significantly, based on local peculiarities.

15. Assessing OPSEC Vulnerabilities:

a. OPSEC Indicators. OPSEC indicators are items of information, observable events, or patterns of detectable activity, whether classified or unclassified. When properly interpreted, OPSEC indicators can provide an adversary an intelligence tip-off that an operation or other activity will occur or yield insights into underlying classified capabilities, system characteristics, doctrine, tactics, techniques or procedures. OPSEC indicators are clues that can cause EEFI disclosures or result in OPSEC vulnerabilities. Vulnerabilities exist if there is a hostile intelligence capability to exploit them. The indicators listed below are neither a complete listing nor do they pertain to every operation. They are provided to help OPSEC officers and activity planners to identify possible problem areas.

(1) *Communications Indicators:*

(a) Change in message volume.

(b) Nets used.

(c) Types or numbers of units on each net.

(d) Prepositioning and testing communications equipment.

(e) Using daily identified or recognized message types, characteristics, call signs, and reporting times; message externals and situation reports (SITREP) requirements indicative of a particular type of activity.

(f) Receiving unusual Armed Forces Courier Service (ARFCOS) shipments.

(g) Implementing MINIMIZE.

(2) *Operations Indicators*:

(a) Stereotyping:

1. Fixed schedules and routes.

2. Standard reactions to hostile acts, maneuvers, procedures, and protective support packages.

(b) Making unusual changes in amount or type of electromagnetic emissions; for example, communications, navigation aids, and radar.

(c) Using unique emitters.

(d) Positioning forces.

(e) Deviating from usual training programs.

(f) Augmenting forces with external assets.

(3) *Intelligence Indicators*:

(a) Intensifying or modifying the use of intelligence-collection resources and warning systems.

(b) Moving special units and equipment.

(4) *Administrative Indicators*:

(a) Issuing unusual types or numbers of TDY orders.

(b) Planning or pre-execution conferences.

(c) Performing unusual special support services, such as transportation, medical care, messing, hotel reservations, trash collections, laundry, or other recreation activities.

(d) Posting special aircrew bus, flight, or maintenance schedules, and notices to airmen.

(e) Cancelling or restricting leave.

(f) Making pyramid recall lists (revealing purpose).

(g) Calling up reserve forces.

(h) Activating new or contingency facilities.

(i) Causing unusual private vehicle traffic or parking.

(5) *Logistic and Maintenance Support Indicators*:

(a) Increasing volume or priority of requisitions.

(b) Prepositioning of equipment.

(c) Enlarging motorpool activity.

(d) Increasing test equipment turnover or calibration.

(e) Advertising nonavailability of base transportation and billeting.

(f) Increasing physical security measures (such as lights or guards around secure facility).

b. OPSEC Indicator Identification. OPSEC officers should be personally involved in identifying those procedures used in their operations and activities that make intelligence collection easier for hostile forces. OPSEC indicator identification by functional specialist and personal initiative is a good method. Other means that can be used include:

(1) OPSEC lesson learned.

(2) Friendly intelligence methods and interests.

(3) Known and postulated hostile intelligence capabilities, methods, and interests.

(4) Common sense assessment of exploitable characteristics of the operation or activity.

NOTE: See AFR 55-30 for additional information.

c. OPSEC Susceptibilities: An indicator that, if exploited, would cause the disclosure of EEFI.

d. OPSEC Vulnerability Identification. OPSEC susceptibilities that are likely to be exploited and cause the disclosure of EEFI, due to hostile intelligence capabilities, are termed OPSEC vulnerabilities (susceptibility x threat = vulnerability). Protective methods or actions to avoid OPSEC vulnerabilities could be costly to resources and mission effectiveness. An accurate intelligence threat assessment is essential to single out those susceptibilities that contribute to real vulnerabilities.

16. Developing Countermeasures. Countermeasures depend primarily on the nature of the threat, the indicator, and the situation. The requirements of the operation and how an indicator relates to success or failure of the operation should be considered. The OPSEC working group can be used to develop recommended countermeasures. Figure 1 is a guide of sample countermeasures. It identifies some techniques that could be used, to include denial and deception. Once these countermeasures are identified and implemented, their success should be evaluated.

17. OPSEC Evaluations. Unit OPSEC posture and the effectiveness of countermeasures are evaluated through OPSEC surveys, OPSEC appraisals, OPSEC self-inspections, and mission success.

a. OPSEC Assessment. This is the process and specific methods for measuring the likelihood that operations and activities can be effectively conducted while denying related EEFI to adversary intelligence collection. It is a tool for evaluatng the effectiveness of OPSEC measures and involves identifying the vulnerability of operations to hostile exploitation in the light of known or estimated foreign intelligence threats. OPSEC assessments are categorized as either surveys or appraisals. Selecting the proper OPSEC assessment method should take into consideration the purpose and objectives of the assessment; the nature of the activity to be assessed; the time-criticality of the assessment results and OPSEC measures; and the availability of OPSEC assessment resources. Broadly stated, the assessment reveals how effective the OPSEC program is. There are advantages for a unit that conducts self-surveys. They are:

(1) Unit personnel become aware of OPSEC vulnerabilities.

(2) The OPSEC office becomes aware of the unit OPSEC vulnerabilities.

(3) The OPSEC officer receives valuable on-the-job training by studying the unit security environment.

(4) Problems can be solved within the unit.

(5) Security programs can be evaluated for results rather than compliance.

b. OPSEC Surveys. OPSEC surveys are explained in detail in the Joint Chiefs of Staff (JCS) OPSEC Survey Planning Guide. Whether the survey is directed by higher authority or from within the unit, there are several principles that should be adhered to:

(1) A survey plan should include purpose, scope, objectives, and data collection plan.

(2) The survey subject should be carefully analyzed to be manageable and within the resources of the survey team.

(3) Surveys are services for the commander and should receive full understanding and cooperation. Surveys are neither inspections nor investigations but tools used to determine the security effectiveness of your unit. The only person hurt by survey results is the hostile intelligence collector.

(4) Team members should instill trust in unit personnel to encourage them to cooperate fully and volunteer information. Surveys should produce results.

(5) Survey teams consist of a variety of different specialties. Surveys by outsiders tend to be

more objective since they are not influenced by, or familiar with, daily unit operations. Every survey team member should remain objective. A successful OPSEC survey requires imagination, cooperation, and participation.

c. **Conducting the Survey.** The survey is an analytical tool for examining an operation and identifying exploitable sources of intelligence by simulating the intelligence-collection process. Hostile agents are smart. They know what they are after and have developed plans to get it, A survey team performs in the same manner. Preparing and planning are the most important aspects of the survey process. The process involves four phases: plan, execute, analyze, and report.
NOTE: Figure 2 is a quick reference for these steps.

d. **Planning.** The survey should be planned well in advance; normally 3 months is adequate. When conducting a survey of your own organization, this time can be reduced based on inherent knowledge of the unit mission. The steps of planning include:

(1) Defining the purpose and scope of the survey. The mission to be surveyed and the specific threat to the operation should be identified (see AFR 55-30 for sources and required lead-times). EEFI should be reviewed for accuracy and used to prioritize survey objectives. This process also establishes survey objectives and determines systems or plans to evaluate.

(2) Identifying support, such as COMSEC monitoring and OPSEC survey team members, needed from agencies outside your unit's span of

TACTIC	OPERATIONAL (PROCEDURAL)	PHYSICAL	ELECTRONIC
DENIAL (Signal reduction)	Night Operations Access control Security classification Media control Use of buildings Cease activity	Opaque Shield (block energy to sensor) Screening Foliage Smoke (diffuse energy) Shadow Soundproofing	Opaque Shielding Terrain masking Cease emission Wire communications Tempest Low probability of intercept (LPI)
BLEND (Contrast reduction)	Traffic flow control Gradual changes Creation of background activity False lighting	Tone down Camouflage materials Pattern/color control Shadow control Insulation (decoupling from the transfer medium) Creation of false background Use of mirrors Reflectors, chaff	Diffuse energy dissipation Emission control Radar cross-section reduction Radar absorbing material Spread spectrum
DISGUISE (Substitution of key characteristics)	Individual movement vs convoy False rumors of intentions Encryption/encoding False indicators	Eliminating/obscuring indicators Incorporating background indicators (altering shapes/sizes) Modifying traces and activity indicators (tire tracks/contrails)	Mask jamming Peacetime modes of operation
DECEPTION (Creation of false identity)	Creation of false activity Leaks of false information False official paperwork False objective/mission	Creation of false items/indicators Creation of characteristics not related to the operation	Creation of false signals Reradiation/reflection False technologys

Figure 1. Countermeasures.

control. Requests for support should be made as early as possible in the planning process. See AFR 55-30 for support sources and leadtime.

(3) Selecting team members. The team chief should be identified. This individual serves as the overall manager of the survey effort and does not take part in daily collection activity. Team members should be selected based on their knowledge in the functional areas to be surveyed and of the threat capability. For example, AFOSI expertise will be required to evaluate the effectiveness of the HUMINT threat to mobility readiness plans; when communications monitoring is planned, the COMSEC Surveillance Mission Supervisor should be a designated team member.

(4) Studying the operation, using plans and directives to obtain an indepth understanding. Even as a unit member, there may be operational relationships with which you are not familiar. Meetings should be held to discuss the study findings and to plan the approach required to accomplish survey objectives.

(5) Notifying the commander and agencies of the survey. Surveys are conducted on an overt basis and the notification may include:

(a) Formal authority to conduct the survey.

(b) Survey purpose and scope.

(c) List of team members and their clearances.

(d) Requested briefings and orientations.

(e) General time span involved.

(f) Administrative support and logistics requirements.

e. Field Survey. A field survey is the execution phase of the survey and involves three steps:

(1) *Arrival and Inbrief*:

(a) The team chief presents the inbrief to the commander and key staff. This briefing sets the tone for all interaction between team and unit members. It stresses that the survey is not an inspection but is a cooperative effort to improve OPSEC effectivensss. This briefing should be informal and include the scope, survey techniques, and threat information developed in the planning phase.

(b) A unit briefing is presented to the survey team to give an overview of the unit's mission, organization, and physical layout. The briefing should clear up any questions that team members may have about the unit mission.

(2) *The Survey*:

(a) The team should be managed to achieve full coverage of the objectives. Team members should operate in pairs to allow sharing of ideas and reinforcing initiatives.

(b) Survey continuity is imperative. Team members should communicate their daily activities to other team members, to prevent duplication of effort. To aid this coordination, a meeting should be held each day of the survey, with all members and members of any other technical support teams present. Additional meetings may be held at the team chief's discretion. The meeting should be held after the day's activities are completed, to discuss findings and compare notes. Tentative findings are formulated and new areas of study developed. The team chief determines if survey

	ACTION	SOURCE
1.	PLAN	
	ACQUIRE EEFI	MAJCOM
	ASSEMBLY SURVEY TEAM	MAJCOM/UNIT
	ACQUIRE FRIENDLY SYSTEM CHARACTERISTICS (AS REQUIRED)	MAJCOM/AFLC
	ACQUIRE FRIENDLY MISSION CHARACTERISTICS	MAJCOM
	ACQUIRE REAL THREAT DESCRIPTION	OSI/ESC/ADCOM
2.	EXECUTE	
	ESTIMATED COLLECTION SUCCESS (EEFI LOST VS. SOURCES)	OPSEC TEAM
	—POSSIBLE COMSEC MONITOR	
3.	ANALYZE	
	RECOMMEND CORRECTIVE MEASURES	OPSEC TEAM
	—POSTULATE IMPACT OF CORRECTIVE MEASURES	
4.	REPORT	
	DOCUMENT/PUBLISH	OPSEC TEAM
	DIRECT CORRECTIVE ACTION	MAJCOM/UNIT
	IMPLEMENT CORRECTIVE ACTIONS	MAJCOM/UNIT

Figure 2. Sample OPSEC Survey Plan.

objectives are being met and if deviations from the data collection plan are required. When all objectives are met, the team completes tentative findings of the survey to be briefed to the unit commander at the exit brief.

(c) Methods of data collection are:

1. Interview—informal, casual.

2. Observation.

3. Study of unit directives.

4. Optional activities:

a. Simulation of HUMINT threat.

b. COMSEC monitoring.

c. Electronic signals analysis, if available (such as, TEMPEST) and electronic security (ELSEC).

(d) Duration of the field survey depends on the depth of study, complexity of organization, and geographic proximity of surveyed facilities. Surveys have been conducted with require more than 30 days while others have required less than a week. The key is knowing the objectives in advance and reaching those objectives. The estimated survey length should be determined during the planning phase.

(3) *OPSEC Survey Exit Brief.* When the survey is completed and initial observation determined, the survey team chief should schedule an exit brief with the unit commander. This briefing is to inform the commander of the major initial observations of the survey, make recommendations, allow corrective actions to begin, and provide feedback for consideration in the final report. The exit brief should be held informally with the commander and members of the staff, if the commander desires their attendance.

(a) The tentative nature of the observations should be emphasized; those which appear firm could be altered after final review of the data.

(b) The final report can require some time to prepare. It is important that an estimated completion date be given to the commander for planning and considering report distribution. Typically, the report is provided directly to the commander who approves further distribution.

f. Example of Final Report Format:

(1) *Overview*:

(a) Historical background.

(b) Purpose, scope, and objective of the survey.

(c) Conduct of survey. Includes a brief discussion of methods used; team composition, degree of unit disruption, and time of survey.

(2) *Intelligence Threat.* Includes data requested from support agencies. Three types of threat should be described:

(a) SIGINT.

(b) HUMINT.

(c) IMINT.

(3) *Summary of Significant Observations*:

(a) *Observation.* You should describe the indicator and associated EFFI which validates the indicator as a susceptibility.

(b) *Threat.* You should describe the threat, as derived from (2)(a), (b), and (c) above, which applies to the susceptibility. If no threat applies, then any potential threat that might apply in the future should be stated.

(c) *Susceptibility or Vulnerability.* This is determined by applying a threat to the susceptibility (threat x susceptibility = vulnerability). This section should be used to discuss any conditions relating to the observation. For example, assumptions concerning threat or susceptibility and effect of EEFI loss on mission. If no threat currently applies, then this item remains a susceptibility.

(d) *Recommendation.* This should be the best corrective action the survey team can devise. If no capability currently exists to correct a vulnerability because of technical or regulation requirements, you should ask for assistance from higher headquarters.

NOTE: Observations should be listed by functional area. If observations are general and affect more than one functional area, they should be listed as general observations and be the last item under observations.

g. OPSEC Appraisal. This is a timely OPSEC assessment conducted in support of a specific operation, activity, or exercise. The appraisal is distinguished from the survey by the timeliness required for threat and vulnerability analysis and the application of OPSEC measures.

(1) The appraisal may be as limited as a simple desk top analysis in response to an operational planner's query, or as extensive as the formation of a multidiscipline appraisal team to support a contingency, exercise, or field test and evaluation event.

(2) The appraisal may be conducted as a follow-up to an OPSEC survey, or it may provide a basis for initiating command or formal surveys.

(3) Appraisal results are provided for timely action by the requesting organization. As in the case of the survey, the commander analyzes the effect of reported vulnerabilities and either takes active countermeasures or accepts the risks posed by the vulnerabilities.

h. Self-Inspections:

(1) The OPSEC officer conducts self-inspections to evaluate OPSEC program compliance

with directives. Attachment 2 is a checklist that can be used as a basis for amplifying directives of your higher headquarters.

(2) Self-inspections do not analyze OPSEC postures but ensure that documentation of the program is completed and supporting activities are conducted.

i. Other Forms of Assessment:

(1) The results of the following examples can be used to evaluate OPSEC posture:

(a) Operational Readiness Inspections.

(b) Management Effectiveness Inspections.

(c) Defense Nuclear Agency Inspections.

(d) Functional Management Inspections.

(e) Exercises.

(2) Other self-initiated efforts, such as desk top security audits and office security audits.

18. Mission Risk Assessment. Risk is based on the comparison of known capabilities of the hostile collector and your ability to deny information or plan for deception. Some indicators may not be denied or disguised and, as such, may give a hostile force a needed piece of information. The level of risk is determined by how extensive the information loss is and how important that information is to mission success. The organization commander compares known or suspected compromise of the operation with the priority of the mission. The commander may decide to proceed using alternative courses of action or accept information losses.

19. Execute and Monitor the Operation. When the commander executes the plan or operation, OPSEC applications should be monitored to determine their effectiveness.

20. Lessons Learned and Feedback. These OPSEC considerations should then be evaluated for use in future operations and plans.

BY ORDER OF THE SECRETARY OF THE AIR FORCE

CHARLES A. GABRIEL, General, USAF
Chief of Staff

OFFICIAL

JAMES H. DELANEY, Colonel, USAF
Director of Administration

ANNUAL OPSEC STATUS REPORT

A1-1. All MAJCOM, SOA and DRU will submit an annual OPSEC Status Report, RCS: HAF-XOE(A) 7106(DD), to HQ USAF/XOEO with an informative copy to HQ ESC/DOO no later than 1 September. The report should consist of command OPSEC activities, problem areas, and lessons learned over a period from 1 July of the previous year and close out on 30 June of the year the report is due.

A1-2. The report should not be limited to HQ element OPSEC activities but should also include noteworthy actions or problems of units within the command. In order to prepare an effective annual OPSEC Status Report, MAJCOM, SOA, and DRU should supplement AFR 55-30 to require subordinate echelons to submit annual OPSEC reports in a timely manner to permit the inclusion of significant items in the command annual report.

A1-3. The annual OPSEC Status Report should also include a forecast of OPSEC initiatives for the next fiscal year. This forecast should consist of scheduled activities as well as recommendation for new initiative at either their level or Air Force-wide.

A1-4. The annual OPSEC report is submitted in the following format:

a. Overview of command OPSEC program status.

b. Training program activities.

c. Summary of OPSEC activities.

d. Problem areas and recommendations.

e. Lessons learned.

f. Forecast of OPSEC activities for the next reporting period.

A1-5. The annual OPSEC report is a formal opportunity to show what your command is doing in OPSEC and to make senior level authorities aware of specific problem areas. The report requires openness and candor to permit it to be a viable tool in the overall Air Force OPSEC program.

OPSEC CHECKLIST

1. Has an OPSEC officer been appointed, in writing, to act as the focal point for all OPSEC matters?

2. Is the unit OPSEC officer knowledgeable about OPSEC concepts, procedures, and objectives?

3. Does the OPSEC officer have the required security clearances?

4. Does everyone know who the OPSEC officer is?

5. Has the name of the OPSEC officer been forwarded to higher headquarters?

6. Is the OPSEC education and training program effective?

7. Does the OPSEC program promote a clear understanding of national, USAF, and MAJCOM concepts and objectives?

8. Does the OPSEC program ensure the active participation and involvement of the entire staff?

9. Are the OPSEC education and training publications listed in AFR 55-30 and MAJCOM supplements thereto available?

10. Are OPSEC education and training publications disseminated to personnel with the appropriated security clearances?

11. Does the OPSEC program include provisions for reviewing plans, OPORDS, directives, and procedures for potential sources of prior knowledge?

12. Has appropriate liaison been established with host or tenant activities on OPSEC matters?

13. Are OPSEC posters displayed in the most visible areas?

14. Are published OPSEC survey reports and studies reviewed for possible application of findings ("Lessons Learned") to local on-going or planned activities?

15. Are the interrelationship of OPSEC, COMSEC, physical security, and administrative security programs clearly understood by unit personnel?

16. Has an OPSEC survey been conducted? If so, when? If not, has one been scheduled or requested?

17. Have positive actions been taken to act on recommendations or to correct weaknesses and deficiencies noted in OPSEC survey?

18. Has the OPSEC officer conducted recent self-evaluations for the following OPSEC indicators:
   a. Subverted military or civilian personnel?
   b. Published or posted unclassified information which is sensitive?
   c. Observable, unique indicators such as special paint or uniforms?
   d. Special field preparations, supply buildups?
   e. Project names, how are they used, with whom are they associated, and how are they communicated?

19. Has the unit developed any special observable operational patterns:
   a. Stereotyped activity?
   b. Preparatory activity?
   c. Increase or decrease of traffic flow and activity such as communications and materials?

20. Are all OPSEC recurring publications reviewed to determine applicability of findings of OPSEC lessons learned?

21. Do the OPSEC considerations for plans include the following:
   a. Purpose and definition of OPSEC?
   b. Multidiscipline threat?
   c. Essential Elements of Friendly Information (EEFI)?

22. Are contingency plans coordinated and distributed only to activities that have a requirement?

23. Are classified materials distributed in a manner that ensures adequate control?

24. Do official and unofficial feedback publications such as squadron, operations or flight newsletters contain sensitive or classified information? If so, are they protected?

25. Do indexes for regulations, BOIs, DOIs,

MOIs, etc., reveal sensitive operations or functions?

26. Do unclassified computer products disclose sensitive mission activity?

27. Are ADP products protected and destroyed as classified waste after they have served their purpose?

☆ U.S. GOVERNMENT PRINTING OFFICE: 1986-490-954/40233