~~CONFIDENTIAL~~

NACSIM No. 4004
DATE: 3 July 1980

National Security Agency
Fort George G. Meade, Maryland

NATIONAL COMSEC INFORMATION MEMORANDUM

COMMUNICATIONS SECURITY SURVEY GUIDE (U)

~~NOT RELEASABLE TO FOREIGN NATIONALS~~

CLASSIFIED BY NSA/CSSM 123-2
REVIEW ON 3 July 2000

~~CONFIDENTIAL~~

National Security Agency
Fort George G. Meade, Maryland

NACSIM NO. 4004
DATE: 3 July 1980

FOREWORD (U)

The ever-increasing capabilities of our adversaries to collect and exploit telecommunications demand that the U.S. Government maintain the strongest communications security (COMSEC) defense possible. By use of sound COMSEC practices and procedures, much of the government-derived classified and unclassified information having a bearing on national security can be protected. NACSIM-4004, COMSEC Survey Guide, outlines techniques for assessing the COMSEC posture of government operations, as a basis for proposing necessary COMSEC improvements.

NACSIM-4004 is intended as a guide for personnel who plan and conduct COMSEC surveys. It is our belief that the performance of COMSEC surveys should be an integral part of all U.S. Military/Civil Agency COMSEC programs. NSA's COMSEC vulnerability assessment personnel continue to rely heavily on this technique when performing COMSEC assessments on behalf of military and civil organizations. We have found that a well planned and executed COMSEC survey is an invaluable aid to defining COMSEC requirements. We strongly encourage the adoption of the COMSEC survey technique by all addressees as a means of bolstering U.S. Government COMSEC programs.

This NACSIM should be retained at proper levels for use by communications, COMSEC, operations security, and other appropriately cleared personnel who may have a need for such information. Additional copies may be obtained from the Director, National Security Agency, ATTN: [redacted]

(b)(6)

[redacted]

HOWARD E. ROSENBLUM
Deputy Director, NSA
for
Communications Security

(b)(3)-P.L. 86-36

OPI: [redacted]or

TABLE OF CONTENTS

PARAGRAPHS: PAGE NO.:

SECTION I - INTRODUCTION

SECTION II - THREAT ASSESSMENT

SECTION III - SURVEY METHODOLOGY

SECTION IV - COLLECTION PROCESS

ALL ENTRIES IN THE TABLE OF CONTENTS ARE UNCLASSIFIED. THIS PAGE IS MARKED TO SHOW THE OVERALL CLASSIFICATION OF THE TABLE OF CONTENTS.

PARAGRAPHS: PAGE NO.:

SECTION V - ANALYSIS PROCESS

SECTION VI - CONCLUSIONS

SECTION VII - RECOMMENDATIONS

SECTION VIII - SURVEY REPORT

ANNEXES

SECTION I - INTRODUCTION (U)

1. (U) Purpose: The purpose of this document is to describe a methodology for conducting COMSEC surveys within Departments and Agencies of the Federal Government. The primary goal of these surveys is to improve the overall operating effectiveness of U.S. Military and Civil users of telecommunications through improved COMSEC practices and procedures.

2. (U) References:

a. (U) ACP 122, Communications Instructions, Security, dated April 1966.

b. (U) National COMSEC/EMSEC Information Memorandum (NACSEM) NO. 5100, Compromising Emanations Laboratory Test Standard Electromagnetics, dated March 1974.

c. (U) NACSEM NO. 4002, Fundamentals of Signals Security, dated July 1975.

d. (U) DoD 5220-22-M, Industrial Security Manual for Safeguarding Classified Information, dated October 1977. (The COMSEC Supplement by the same title was previously published in April 1975).

e. (U) Presidential Directive/NSC-24, Telecommunications Protection Policy, dated 16 November 1977.

f. (U) Executive Order 12036, United States Intelligence Activities, dated 24 January 1978.

g. (U) National Communications Security Directive, dated 20 June 1979.

h. (U) National COMSEC Instruction (NACSI) No. 4005, Safeguarding and Control of Communications Security Material, dated 12 October 1979.

3. (U) Definitions: For purposes of this document, the following definitions apply:

a. (U) Communications Security (COMSEC): COMSEC means protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emission security) to electrical systems generating, handling, processing, or using national security or national security-related information. It also includes the application of physical security measures to COMSEC information or materials.

(1) Cryptosecurity. The component of COMSEC which results from the provision of technically sound cryptosystems and their proper use.

CLASSIFIED BY NSA/CSSM 123-2
REVIEW ON 3 July 2000

(2) Transmission Security. The component of COMSEC which results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. (These other means include traffic analysis, signal analysis, emitter identification (radio fingerprinting), direction finding, imitative communications deception, intrusion, meaconing, and jamming).

(3) Emission Security. The component of COMSEC which results from all measures taken to deny unauthorized persons information of value which might be derived from interception and analysis of compromising emanations from crypto-equipment and telecommunications systems. (TEMPEST is used synonymously with the term "compromising emanations".)

(4) Physical Security. The component of COMSEC which results from all physical measures necessary to safeguard COMSEC material and information from access thereto or observation thereof by unauthorized persons.

b. (U) Telecommunications: Means the transmission, communication, or processing of information, including the preparation of information thereof, by electrical, electromagnetic, electromechanical, or electro-optical means.

c. (U) National Security: Means the national defense and foreign relations of the United States.

d. (U) Operation: Means any U.S. Government Military/Civil endeavor, activity, or function in which telecommunications are used to communicate government-derived classified information and government-derived unclassified information relating to the national security.

4. (U) Background:

a. (U) Before the advent of COMSEC surveys, communications monitoring and analysis had been one of the principal means of assessing COMSEC within the U.S. Military and certain Civil activities. There are, however, certain limitations to this approach. Under the monitoring concept, only a small sampling of communications associated with an operation or function is normally examined. Although this may be useful to an operations chief as a means of estimating the types and volumes of potential intelligence information revealed by his/her communications, the COMSEC problems are usually not defined in sufficient detail to suggest the best solution. Further, with the monitoring and analysis approach, corrective actions usually occur after the fact.

b. (U) The best solution is one that will allow COMSEC problems to be corrected before an operation begins or at least as soon as possible after they are detected. The COMSEC survey approach provides such a solution. Rather than identifying the symptoms of COMSEC weaknesses, as is often the case in monitoring and analysis, a COMSEC survey seeks to identify the causes of and provide a basis for eliminating the circumstances which lead to COMSEC violations. However, when conducted in support of a COMSEC survey, monitoring and analysis can still be helpful in developing empirical information and necessary technical data which can aid in validating overall survey findings.

5. (U) Survey Concept:

a. (U) A COMSEC survey is a systematic means of rapidly identifying and eliminating communications practices and procedures which could serve as sources of enemy intelligence, including improper safeguarding of COMSEC materials. In order to accomplish this, all communications associated with an operation must be examined, with particular attention focused on the means of communication, the content of plain-language information transmitted, and the use of cryptographic systems. Interviewing of personnel by the survey team is an essential step in performing the overall communications examination. As nearly as possible, the survey team should simulate the adversary's role when assessing the vulnerabilities of the communications. However, when assuming the adversary's role, care should be taken to refrain from making unfair assessments based on information and circumstances that only a "friendly" would know and be capable of exploiting.

b. (U) Although there is no formal requirement to identify and eliminate noncommunications sources of enemy intelligence, such as stereotyped patterns of operational activity, appearance of special purpose units or weaponry, logistics buildups and prepositioning of support units etc., such sources of intelligence may be identified in the course of a COMSEC survey and should be called to the attention of appropriate authorities. These sources of enemy intelligence are normally those for which the broader-scope operations security (OPSEC) surveys are designed to detect.

NOTE: OPSEC measures are designed to protect U.S. Government and Allied operations against the all-source hostile intelligence threat stemming primarily from enemy human intelligence (HUMINT), photographic intelligence (PHOTINT), and signals intelligence (SIGINT). SIGINT threats are composed of communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). COMSEC measures are primarily designed to protect against COMINT and FISINT plus those HUMINT attacks designed to collect COMSEC information and materials. COMSEC, therefore, is a major component of OPSEC and the examination of COMSEC factors has variously been estimated to compose upwards to 75 percent of the overall effort involved in an OPSEC survey. At any rate, whether performed independently or in support of a larger OPSEC survey effort, COMSEC surveys should always be thought of as being a primary means of bolstering the overall OPSEC posture of a U.S. Government or allied operation.

c. (U) To eliminate COMSEC weaknesses that could serve as sources of enemy intelligence, a COMSEC survey must begin with the planning stage of an operation and continue through the execution and post-evaluation stages. Central to this concept is recognition of the fact that communications are normally essential to the conduct of operations.

A COMSEC survey seeks to complement these operations by ensuring that the communications involved are conducted as securely as possible.

d. (U) The chief of the activity being surveyed must be fully informed of the intent and scope of the survey and full cooperation of the chief should be obtained. Only in this atmosphere can team members perform their tasks with regard to the above stated goals.

SECTION II - THREAT ASSESSMENT (U)

6. (U) <u>Threat Factors</u>: The need for a COMSEC survey is directly related to the hostile threat. The impact of a survey is enhanced if the hostile threat to the communications of a given operation can be defined. Definition of threat also aids in the selection and prioritizing of activities to be surveyed. When assessing the hostile intelligence threats, COMSEC survey planners should examine all intelligence data which may bear on the problem to determine:

a. (U) For hostile land-based collection facilities:

(1) Unit location and function/purpose (e.g. COMINT, FISINT, etc.)

(2) Whether fixed site or mobile. (If mobile, date set up)

(3) Equipment.

(4) Antenna orientation.

(5) The technical capability and sophistication of the nation concerned.

b. (U) For hostile seaborne collection platforms:

(1) Positions of all known or suspected military, scientific, and commercial vessels engaged in enemy collection efforts.

(2) Home port and normal area of operation.

(3) Collection capability.

(4) History of collection operation.

c. (U) For hostile airborne collection platforms:

(1) Type and number of units/aircraft involved.

(2) Home base and normal operating area.

(3) Flight routes and schedules.

d. (U) For hostile intelligence satellites:

(1) Specific satellite and function.

(2) Its orbit.

(3) Estimated hourly position.

e. (U) For HUMINT threats:

(1) Legal residence of potential HUMINT agents (embassies, news agencies, etc.)

(2) Illegal residences (clandestine facilities, roving land vehicles, etc.) and covert/overt agents identified through available intelligence sources, e.g., DIA, CIA, FBI, etc.

(3) Potential terrorist activity, mob violence, and the like, which would jeopardize COMSEC physical security.

f. (U) For all hostile collection platforms/facilities:

(1) Collection equipment capabilities and frequency coverage.

(2) Unit's ability to exploit information on a real-time basis.

(3) Probable target(s) of each collection unit.

7. ~~(C)~~ Adversary Capability: Exact knowledge of the success of any hostile intelligence effort is closely guarded; however, it must be assumed that the enemy is capable of intercepting all types of transmissions. It follows then that all communications not adequately secured, particularly plain-language voice transmissions, are vulnerable to exploitation. As an example, Warsaw Pact nations have ideal geographic positioning to monitor NATO and European-based U.S. communications. The overall quality of their COMINT effort is reportedly high, particularly against unencrypted voice communications. There are also strong indications of a high degree of collaboration among the Warsaw Pact nations and, for all practical purposes, this COMINT effort must be considered an extension of the Soviet threat to U.S. and NATO communications.

8. (U) Hostile Interest in U.S. Operations:

a. (U) An enemy's intelligence interest in a particular U.S. operation could stem from a number of reasons. Two of the more important ones are: (1) the intelligence value of the communications; and, (2) the vulnerability of the communications to interception and exploitation. These considerations, plus those factors discussed in the foregoing paragraph, combine to form the basis for estimating the enemy threat.

b. (U) The above considerations will require survey planners and survey team members to extensively review the functional areas (contained in OPORDS/OPLANS, RDT&E test schedules, etc.) of a given operation to become familiar with the mission. From these documents, planners and team members should be able to acquire insight into the most important operational activities, the types of information of intelligence value likely to be communicated, and the approximate times the most important transmissions occur.

9. (U) Intelligence Reports: Intelligence reports of past enemy intercept activities and successes against U.S. Military/Civil targets can assist survey planners in determining hostile interest in particular targets, thus simplifying the task of choosing an operation to survey. Also, the reports can help promote a receptive attitude on the part of operational commanders and civil agency managers regarding the need for COMSEC surveys. By pointing out how past operations have been exploited as a result of COMSEC weaknesses, intelligence reports can convince a commander or civil agency manager that his/her own communications are equally vulnerable.

10. (U) Presumed Interest: When positive proof of enemy interest is lacking, presumed interest becomes the basis for conducting a COMSEC survey. The intelligence value and vulnerability of the communications to interception and exploitation have been mentioned as factors that might stimulate hostile interest in a particular operation. Determining overall COMSEC vulnerability is, of course, the goal of the survey itself. To determine if a survey is warranted, however, only a presumption of vulnerability is sufficient. If available, monitoring and analysis reports of similar past operations can be helpful in confirming suspicions of vulnerability of a particular operation's communications.

SECTION III - SURVEY METHODOLOGY (U)

11. (U) Approach: A COMSEC survey team uses a step-by-step, fact-finding process much like that used by any group or individual engaged in a problem solving effort. A number of actions, questions, and analytical approaches must be considered when examining the communications facilities, procedures, and activities of an operation. Essential steps in the process include:

a. (U) Collection and documentation of all data pertinent to the examination.

b. (U) Processing and analysis of the collected data.

c. (U) Determining findings and conclusions.

d. (U) Proposing recommendations for corrective actions.

e. (U) Preparation of final survey report.

12. (U) Investigative Procedures:

a. (U) Because of the varied functions and communications activities of each operation, standardization of checklists and investigative procedures is nearly impossible. Consequently, survey teams are encouraged to expand procedures in this document and develop checklists and procedures applicable to the survey target. The complexity and scope of the operation may require the formation of a special augmentation team composed of operational personnel from the entity being surveyed. This team must be thoroughly briefed by the visiting COMSEC survey team leader and totally integrated into the overall team structure.

b. (U) All collection and evaluation of information must be accomplished with care to avoid overlooking or discarding essential information. Although it may not be feasible to attempt to collect all friendly communications related to the operation, sufficient data should be collected during an examination to permit thorough analysis of those communications considered most relevant to the conduct of the operation.

13. (U) Team Composition:

a. (U) Considering the sophisticated intelligence collection techniques of some hostile nations, the ideal survey team should be composed of communications and COMSEC personnel and, when available, operations and intelligence personnel to augment the team. Very often, the operations personnel on the team will be designated from within the operation being surveyed. Having all four skills available assures the broadest coverage, especially during the analysis phase when the assorted data has to be analyzed and meaningful conclusions drawn. However, if operations and/or intelligence personnel are not available to augment a team, a very effective, in-depth survey can still be conducted with just communications and COMSEC personnel.

b. (U) Ideally, each member should possess broad knowledge of all communications systems and related operating procedures, cryptographic systems being used and available for use, and sufficient knowledge of the overall operation being surveyed. The two most important capabilities desired in team members are: (1) the ability to detect a real COMSEC weakness; and, (2) the ability to recommend the proper solution for correcting that weakness. These capabilities are developed with experience. Therefore, the most experienced personnel with the desired skills should be considered first when establishing survey teams. Members should be encouraged to take part in as many aspects of the survey as time permits regardless of their background experience.

c. (U) Emission security (TEMPEST), although a vital component of COMSEC, is a more specialized field requiring unique training, equipment, and laboratory assessment techniques. Consequently, because of its specialized nature, it is believed that the capability to perform extensive TEMPEST vulnerability assessments during a routine COMSEC survey will be beyond the capability of most COMSEC survey teams. However, when such expertise is present, obvious TEMPEST hazards, e.g., noncompliance with prescribed RED-BLACK installation criteria, should be kept in mind during a COMSEC survey. Should any cursory TEMPEST assessments be made during a routine COMSEC survey, these should certainly be noted and then followed up later on by a TEMPEST inspection team put together solely for the purpose of gathering TEMPEST data necessary for conducting laboratory testing at a later date. Reference b., should be consulted for further information relative to TEMPEST vulnerability assessment techniques.

d. (U) Technical surveillance countermeasures (TSCM) sweeps to detect the presence of clandestine listening and recording devices are also not normal components of a COMSEC survey team, but are potential adjuncts. However, survey teams should ascertain when TSCM sweeps were last conducted and determine whether a new sweep is currently required.

14. (U) Size and Capability of Team:

a. (U) The size of the team depends upon the type and scope of the operation being surveyed. If it is a military operation, a mix of officers and enlisted personnel is normally desirable when forming a survey team. The designated team chief should be capable of supervising all phases of the survey dealing with collection, analysis, and the formulation of conclusions and recommended actions for improving the COMSEC of the operation. In accordance with their background, the other members should be capable of providing assistance in various COMSEC areas involving transmission security, cryptographic security, emission security, and physical security of COMSEC information and materials. They should be well versed in the fundamentals involving the use of all radiotelephone, teletype, CW, data, facsimile, and conventional telephone communications systems being used in the operation, as well as any associated computer security applications.

b. (U) Civil agency COMSEC survey teams or civilians serving on a predominantly military team should possess the same survey capabilities as their military counterparts cited above.

15. (U) Teamwork Approach:

(U) Teamwork is a vital factor in the successful conduct of a survey. Rather than conducting interviews individually, members should work in teams of two or three each and conduct the interviews as a unit. This approach allows each member to be used more effectively and also allows teams to be "tailored" to specific tasks when required. Because there may be numerous elements to be visited during the survey of a large operation, each group should visit different elements. During the survey, the groups should periodically meet and discuss their findings.

16. (U) Predeployment:

(U) Before commencing the actual survey, team members must first obtain a basic understanding of the operation to be examined. All available informational documents, such as applicable OPORDS/OPLANS, test schedules, COMSEC annexes, intelligence reports, classification guides, command CEOIs/SOIs, and operational SOPs, must be reviewed in detail. As a result of this review, some clarification may be required before deployment when the reviewed information is counter to that previously thought to be true. Along these same lines, review of this information can also serve as a basis for discerning that the information developed during the survey differs greatly from that contained in the SOPs and other reviewed operational documents. It can be seen that this initial review is very important to the success of the survey; therefore, it should be conducted with care. From past experience, team members should already be familiar with those basic guidance documents that pertain to proper communications procedures and COMSEC practices. If not, study of these materials should be accomplished before deployment.

17. (U) Itinerary:

a. (U) The team should be aware of all commands and/or civil organizations involved in the operation, including those in minor supporting roles, to ensure that all potential sources of enemy intelligence information are being considered. Depth of contractor involvement must be ascertained, when relevant, in order that this potentially lucrative source of intelligence information is not overlooked as a possible target of hostile collection units. Reference d., contains basic COMSEC guidance applicable to contractors and should be consulted for additional information concerning contractor involvement in U.S. operations where classified/sensitive information may require COMSEC protection.

b. (U) The team should determine and coordinate with the supported activity all locations or activities to be visited, dates and times of planned visits, and expected completion dates of each examination. However, the list of locations may have to be changed during the course of the survey as the team becomes more familiar with the operation. The list should include the headquarters of all subordinate elements of the operation and the identity of all military units and/or civil elements that will be directly involved. By visiting all locations, team members may discover unexpected vulnerabilities which, in turn, may require visits to other locations not previously identified. Prior authorizations should be granted COMSEC survey teams to "follow-up leads" as the survey progresses and to amend their planned itineraries accordingly to accomplish this.

18. (U) Support Requirements:

a. (U) Concurrent with notifying the operational chief of the objectives and scope of the survey, clearances of team members, expected arrival dates, schedule of events, and major points of interest, the team should also make known any team support requirements. Typical support requirements include:

(1) Land, sea, and air transportation.

(2) Team quarters, working spaces, conference sites, etc., while in the field.

(3) Local communications, COMSEC, operations, or intelligence personnel who may be called upon to augment the visiting survey team.

(4) Other logistical support.

b. (U) The message or letter to the supported activity, outlining the above support requirements, should conclude with a request by the team leader to brief the operational chief and his staff chiefs upon arrival at the activity.

SECTION IV - COLLECTION PROCESS (U)

19. (U) Deployment: Upon arrival, the team leader should brief the operational chief and selected staff members on specific aspects of the survey including primary objectives, methodology involved, and reasons why this particular activity or operation was chosen as a survey target. This opportunity can also be used to mention any additional team support requirements, additional locations to be visited, and any changes to the previously announced survey schedule. Following the team leader briefing, the visiting team should receive an introductory briefing from the activity's operational chief or staff for purposes of:

a. (U) Providing the team with greater understanding of the overall operation.

b. (U) Enabling the team to correct any misunderstandings resulting from review of the OPORDS/OPLANS, test schedules, etc.

c. (U) Enabling team members and operational personnel to exchange general viewpoints regarding the operation, communications involved, and the forthcoming survey itself.

20. (U) Clarification of Objectives: It is imperative that the operations chief and the survey team leader reach a clear understanding, from the outset, regarding the main objective of the survey. Since the goal is to increase the overall operational effectiveness of the activity through improved COMSEC measures, the team leader should emphasize that all conclusions and recommendations will be aimed at assisting the activity to achieve that goal. It should also be pointed out that all involved units associated with the operation will be given an opportunity to comment on all survey findings during the team's exit briefing and, if appropriate, to identify corrective actions already taken or planned before the final report is issued.

21. (U) Task Assignments: Having been assigned a particular function to examine, each survey team group must identify all the communications activated in support of that function during the planning, execution, and postexecution phases of the operation. All relevant communications must be traced from their origin to the final addressee and, where they cross operational or national boundaries, arrangements must be made with appropriate authorities to identify the path of the communications to their ultimate destination.

22. (U) COMSEC Weaknesses:

a. (U) Once on location, team members should concentrate on identifying basic COMSEC weaknesses. These should be identified by using the following methods:

(1) Determine what is classified or sensitive about the operation.

(2) Identify specifically how the classified or sensitive aspects of the operation are communicated.

(3) Determine whether adequate COMSEC protection is given to these classified or sensitive aspects, including physical security protection.

b. ~~(C)~~ Some of the more important weaknesses include the following:

(1) Transmission of sensitive, plaintext information over unprotected circuits, especially radiotelephone circuits.

(2) Mixing plain text with cipher or encoded text when not authorized.

(3) Using static frequencies and call signs.

(4) Using international call signs when not authorized.

(5) Using call sign suffixes that divulge net structure and order-of-battle information.

(6) Using unsecure "homemade" manual cryptosystems, e.g., operations codes, numeral codes, and authenticators.

(7) Using authorized COMSEC equipments and materials improperly. Examples include:

(a) Operating crypto-equipments inadvertently in the clear.

(b) Leaving ORESTES (KW-7) circuits in the "idle" mode.

(c) Using "short-term security" codes to encode information which requires "long-term security".

(d) Excessive use of an operations code to encode pro forma-type messages.

(e) Using numeral codes for spelling purposes.

(f) Excessive use of general operations codes for spelling.

(g) Using certain crypto-equipments to process communications for which they were not designed.

(8) Association of call signs or exercise code words with their meanings.

(9) Increasing the volume of cipher messages during special phases of an operation.

(10) Stereotyped message externals such as address groups, formats, routing indicators, precedence, and date/time groups.

(11) Operator chatter.

(12) Nonuse of available cryptographic systems.

(13) Failure to encrypt UTM grid coordinates.

(14) Violation of the need-to-know principle regarding distribution of received messages or other COMSEC information.

(15) Nonadherence to sound cryptomaterial handling and accounting procedures.

(16) Use of insecure facilities and/or procedures to destroy classified, superseded COMSEC material.

c. (U) Each COMSEC weakness cited above can either be exploited directly or else can serve as an overriding factor which can lead to possible future exploitation. When a number of these COMSEC weaknesses exist within an activity, it becomes only a matter of time before hostile intelligence units are able to obtain information about the operation. In some cases, sufficient information may be divulged to allow hostile collectors to accurately identify the nature and success of specific RDT&E projects, predict future U.S. Government actions and intentions, and successfully degrade U.S. operations in general.

23. (U) Interviewing Operational Personnel:

a. (U) Effective interviewing is crucial to the success of the COMSEC survey. Communications, COMSEC, operations, intelligence, staff, and other action officers who originate, receive, or relay communications, should be interviewed. Rather than rely on memory, careful notes should be taken by team members during the interviews.

b. (U) The questions asked of operational personnel should be carefully formulated to obtain positive, conclusive answers. To do this systematically, team members should prepare most of their questions in advance of the interviews or, at least, have in mind the general types of questions they need to ask. This not only saves time and avoids ambiguous and unproductive questions, but allows the team to ask questions that are more in line with the duties of the person being interviewed. In short, regarding the question and answer sessions, careful preparation by team members will pay great dividends later on in terms of desired survey results.

c. (U) Team members should assure interviewed personnel that any information provided will be handled on a "nonattribution" basis, i.e., individual names will not be associated with specific findings or COMSEC problems identified in the final report. This approach is intended to encourage all personnel interviewed to speak freely so that they may provide other valuable information in addition to answering direct questions. This additional information, when correlated with other data, may result in the detection and elimination of COMSEC problems previously unsuspected.

24. (U) <u>On-site Observations</u>:

a. (U) Participation in the actual operation is an invaluable part of the survey, as it allows the team to observe and listen to what actually occurs rather than rely solely on information obtained through interviews and document reviews before arrival on site.

b. (U) The communications must be observed as they normally occur in order to make realistic judgments and prescribe practical solutions for correcting COMSEC weaknesses. Consequently, the activity being surveyed should avoid implementing special practices and procedures simply for the benefit of the survey team. In essence, unless the communications are assessed as they normally occur, the purpose of the survey is defeàted.

25. (U) <u>Developing the Data Base</u>:

a. (U) <u>General</u>: From information obtained during the predeployment phase, interviews and on-site observations, the survey team should acquire sufficient information to establish a detailed narrative and graphic data base. The basic categories of information required in the data base include operations, communications, COMSEC, and pertinent intelligence information having a bearing on the results of the survey.

b. (U) <u>Operations</u>: This section of the data base should identify all elements/activities participating in the operation, their major actions or functions, and the sensitive aspects of each. It should also identify whether these actions occur during the planning, execution or postexecution stages of an operation, and pertinent order-of-battle information, if a military operation. All information in this section becomes very important during the analysis phase when the team is trying to determine if correlations exist between certain friendly transmissions and those known or suspected actions of adversary intelligence collectors.

c. (U) <u>Communications</u>:

(1) This section should contain a listing of all tactical and strategic networks/circuits routinely activated in support of the operation. Since the communications being examined are those consistently used by elements of the operation, the survey is mainly concerned with identifying methods and procedures that are officially authorized or at least widely practiced, but which are technically unsound from a COMSEC standpoint.

(2) Net diagrams of the primary circuits should be constructed and complete information sheets prepared on each system. 'Accurately constructed net diagrams and accompanying information sheets are unsurpassed as analytical tools. Consequently, they should be prepared with care.

In addition to aiding survey teams to better understand the working relationships between net members (i.e., who talks to whom, when, and about what, etc.), net diagrams can also provide a clearer perspective of the overall operation. Also, by graphically displaying the net information, survey teams are better able to identify COMSEC weaknesses and depict them in a more obvious light.

(3) Although the volume and type of information pertaining to each communications system may differ from one operation to the next, there are certain basic types of information that should be identified for every system. These include:

(a) Net purpose: command/control, adminitrative, logistical, air-ground, etc.

(b) Communications mode: voice, teletype, data, facsimile, etc., and whether transmission is by radio, wireline, or a combination of both.

(c) Net control station and list of all subscribers; and whether the net is operated as a "free" or a "directed" net.

(d) Order of call up and acknowledgement.

(e) Station call signs and net collective call.

(f) Net/circuit designator.

(g) Typical message externals such as address groups, routing indicators, precedence, etc., and whether format is "pro forma."

(h) Normal volume and sensitivity of all plain-language communications.

(i) Times most transmissions are made relative to planned and ongoing activities of the operation.

(j) Usual quality of transmissions and receptions.

(k) Any unusual communications instructions or operating procedures relative to such things as call ups, sign offs, and operating signals.

(l) Identity of any net/circuit being used for other than intended purpose and reason why; determine volume and type of traffic passed.

(m) Method of handling unclassified versus classified messages.

(n) Procedures for rerouting traffic when primary circuits are inoperable.

(o) List any new communications systems or improvement programs in progress or planned, including training programs.

(p) Make note of other nonelectrical means of communications being used such as courier and flashing light.

(4) For all radio nets, determine:

(a) Normal operating frequency and tuning range of transmitter.

(b) Power output of transmitter under normal conditions.

(c) Type, height, directivity, and propagation pattern of antenna.

(d) Topographical features of transmitter site(s).

(e) Type of emmission, such as SSB, AM, or FM.

(f) Percent of transmissions made during the day versus at night.

(g) If microwave, determine paths between stations.

(h) Any other factors bearing on the interceptability of the signal.

(5) For landline circuits, determine:

(a) Routing of primary and alternate circuits, and terminal points of each, and whether the routes pass through the territory of hostile governments.

(b) System/circuit designators.

(c) Method of switching (automatic versus manual patching) and list of switching centers.

(d) Type of cable and criteria used for installing.

(e) Whether it is a short- or long-haul system.

(6) Even though an organization's communications are believed to be secure, some knowledge of the operation may still be regularly indicated to an enemy by some unsuspected means, e.g., its communications operating patterns and procedures. The source of tip-off may be the improper use of secure systems or possibly that the transmission patterns and emitter identifications are such that an enemy has learned to predict forthcoming events. This is why all communications transmissions related

to an operation must be subjected to a detailed examination if all sources of enemy knowledge resulting from these communications are to be eliminated.

(7) Although the effectiveness of the search for sources of hostile intelligence is directly proportional to the thoroughness of the communications examination, there may be some justification for deferring the review of some of the communications involved. In cases where it might be impractical to examine the entire communications facilities and practices of an operation, the examination should be directed first at those activities and transmissions that experience and/or intelligence reports have identified as known or suspected sources of hostile intelligence information.

(8) Normally, hostile intelligence collectors need reliable and fairly constant sources of information. These sources, because they may be based on weaknesses resulting from the operation's use of traditional or approved practices, may require special evaluation to identify and eliminate. Where traditional practices are slow to change, it is likely that there also exists a lack of appreciation for the sophisticated communications intercept and processing techniques of all modern, adversary nations. For this reason, all personnel involved in communications activities must be properly indoctrinated regarding the hostile threat to U.S. Government communications.

d. ~~(C)~~ COMSEC Measures Employed: This section should contain all information related to the cryptographic, transmission, and physical security aspects of each communications system. Because emission security aspects are normally beyond the scope of most COMSEC survey teams, no attempt is made to include these factors in the following subparagraphs. Essential COMSEC information includes:

(1) Types of secure equipment in use (voice, teletype, data, etc.), whether they are used on-line or off-line, and whether the on-line systems used provide traffic-flow security.

(2) Procedures for employing each COMSEC system; list all guidance documents and directives having a bearing on the use of each system.

(3) The purpose of each secure link, circuit or net; command/control, diplomatic, local operational, etc., and whether it is air-air, air-ground, ground-ground, or ship-to-shore, etc.

(4) All authorized manual cryptosystems (authenticators and codes, etc.) available for use and the sensitivity of information being encoded/enciphered in each.

(5) Types of unauthorized "homemade" codes in use and volume of classified information encoded in each system.

(6) All protected wireline or fiber optic distribution systems used in support of the operation and types of information passed over each circuit.

(7) All communication systems employing changing call signs, suffixes, and frequencies and the specific changing call sign system employed.

(8) Nets/circuits affording only partial security.

(9) Techniques for countering enemy meaconing, intrusion, and jamming.

(10) All cryptographic systems in the planning stage; list type of system, intended purpose, expected installation date, total subscribers, and whether holders will be national or multinational.

(11) A description of each communications facility and COMSEC vault entry control system and physical safeguards (e.g., guards, fences, and alarms).

(12) The adequacy of all destruction facilities available to the COMSEC custodian.

(13) Clearance status of all personnel engaged in handling, or who have access to, classified messages and related information.

(14) Current regulations dealing with physical security aspects of the operation's COMSEC facilities and materials (e.g., SOPs).

e. ~~(C)~~ Hostile Intelligence Considerations: This section should include information, in as much detail as possible, on all adversary SIGINT/HUMINT activities that might be directed at the operation under study.

(1) An identification of all known, suspected, or potential enemy efforts to obtain information about this or a similar operation should be documented. If known, the successes attached to those efforts should be included.

(2) The threat assessment portion should include all means to collect and exploit information, relative to the targeted operation, by electronic intercept and visual surveillance and any hostile efforts to subvert personnel assigned to the operation. The risk of any hostile overt/covert agent being detected should be ascertained, if possible.

(3) The collection capability and real-time analytical capability of hostile COMINT units should be assessed.

(4) Those activities within the operation considered to be primary enemy collection targets should be identified and ranked in accordance with the known or presumed priority of importance the enemy has placed on each target.

(5) The amount of publicity given the operation as a result of U.S. or Allied press releases, radio and television coverage, etc., should be determined. Also, a brief assessment of the publicity given any previous operation of a similar type should be prepared.

(6) Any information developed as a result of past friendly COMSEC monitoring and analysis or SIGINT activities which would aid in verifying hostile interest in the operation should also be made a part of the hostile intelligence data base.

NOTE: It is recognized that some of the above considerations are normally thought of as being factors more closely related to OPSEC surveys than pure COMSEC surveys. Nevertheless, because so many of these factors are so intrinsically related to both OPSEC and COMSEC, there is no easy way to separate them into an "either/or" category in every situation. Accordingly, when developing the "hostile intelligence considerations" data base, nothing should be discarded outright; one piece of seemingly unrelated information may ultimately lead to another key finding which does relate directly to a COMSEC problem.

f. (U) Processing of Collected Information:

(1) All collected data should be assembled for documentation and processing at a central location, and displayed in a manner that will aid the search for COMSEC weaknesses. The senior COMSEC person attached to the team would normally direct the processing, but this is optional and could vary from survey to survey.

(2) To facilitate the "analysis, conclusion, and recommendation processes," there are many ways of arraying the collected data. The manner chosen by a survey team will depend on the type of operation surveyed and personal preference of team members. Examples of several such techniques for doing this are shown in Annex A, Matrices 1-4, which have direct relationships to the analytical questions posed in Annexes B-E.

(3) All personnel involved in the collection effort should be present throughout the processing phase, so that any discrepancies in the collected information can be immediately resolved. In addition to net diagrams, organizational flow charts should be prepared, as these become very useful when determining whether correlations exist between certain stereotyped patterns of transmissions and specific operational functions. Once definite correlations have been established, it becomes an easier task to predict which transmissions would most likely serve as a source of tip-off to the enemy regarding forthcoming events, thereby further aiding their collection efforts. Such a prediction becomes even

more valid when the transmissions involved, in addition to being stereotyped and always correlated with certain activities, are accepted as being highly vulnerable to interception and exploitation due to the mode of communication used, such as plain-language radiotelephone. In a military operation, where the element of surprise may be essential to the success of the operation, the control or elimination of communications tip-off indicators would be the primary goal of a COMSEC survey.

SECTION V - ANALYSIS PROCESS (U)

26. (U) General:

a. (U) The establishment of the survey data base marks the end of the collection phase of the survey and begins the analysis phase. The information listed in the foregoing data base sections should not be considered the only information that may be required during the analysis phase, as no attempt was made to include therein every conceivable piece of information that might be relevant. The list does, however, represent most of the essential types of data required for thorough analysis.

b. (U) The analysis phase requires a much more sophisticated approach than the collection phase due to the increased number of judgments that have to be made. Consequently, to effectively evaluate the information in the data base, a judicious method of analyzing the data must be developed and logically applied (see Annex A, Matrices 1-4, for examples).

c. (U) It has already been mentioned that the COMSEC situation should be assessed from the adversary's viewpoint, as it is the adversary's wherewithal that, in reality, decides whether a real threat to the COMSEC of the operation exists or not. Also, when performing analysis and contemplating solutions to particular COMSEC problems, the analyst must consider the operation as a whole and not aim only at improving the security status of a small portion of the operation. This may be difficult at times if the COMSEC problems are complex and widespread, but an attempt must still be made in order to assure that all factors having a bearing on the security of the operation have been considered. It is possible that, while endeavoring to "fix" a portion of the COMSEC problems, a new and significant security problem could be inadvertently created, unless all ramifications of the operation have been considered when recommending COMSEC corrective measures.

27. (U) Objectives:

a. (U) All COMSEC aspects of the communications involved must be subjected to a series of analytical questions designed to obtain the types of responses that will lead to conclusive findings. The types of questions should, as much as possible, bear a relationship to the Essential Elements of Friendly Information (EEFI) to which the operation wants to provide maximum COMSEC protection. It should be noted that the activity being surveyed, and not the COMSEC survey team, is responsible for establishing and classifying the EEFI list.

b. (U) Broadly speaking, the objectives of the analytical effort are to determine:

(1) The type, volume, and sensitivity of all operational information being made available to hostile intelligence collectors as a result of the operation's communications and COMSEC posture.

(2) The identity of those COMSEC weaknesses directly or indirectly responsible for classified or sensitive operational information being made available.

(3) What steps can be taken either to prevent hostile collection and exploitation successes or make such efforts more difficult.

28. (U) Transmission Security Analytical Questions: This category of questions should try to determine how vulnerable the transmissions are to enemy interception, traffic analysis, signal analysis, emitter identification, direction finding, imitative communications deception, intrusion, meaconing, and jamming. See Annex B for example questions in this category.

29. (U) Cryptographic Security Analytical Questions: Questions in this category should aid in determining the total cryptographic protection being afforded the operation's communications. See Annex C for example questions.

30. (U) Physical Security Analytical Questions: Questions in this category should attempt to clarify how well the communications and COMSEC facilities, equipments, and related materials and information are being physically protected. See Annex D for the types of questions in this category.

31. (U) General COMSEC Analytical Questions: The questions posed in Annexes B-D cited above are designed to analyze and detect specific factors that could adversely affect the COMSEC status of an operation. Unlike the foregoing questions, the general COMSEC questions relevant to this subsection are designed primarily as a means of determining overriding factors that created or substantially contributed to conditions that allow specific COMSEC weaknesses to prevail. Since questions of this type are decidedly more subjective than those in Annexes B-D, the opinions formed will mainly be based on generalized impressions rather than supportable facts. Accordingly, analysis produced as a result of these questions should be used mainly as amplifying information and not as conclusive evidence of COMSEC vulnerabilities. See Annex E for the types of questions fitting this general category.

32. (U) Development of Additional Analytical Questions:

(U) The types of questions eventually developed by each survey team will depend largely on the type of operation and complexities involved. Consequently, the questions in Annexes B-E represent only a partial listing of an endless number and type of questions that may be asked. For aid in developing additional questions, References a. through d. and h. are recommended as sources of ideas. Analytical questions relative to emission security (TEMPEST) have been omitted due to reasons previously expressed. Should a survey team desire to formulate such questions, Reference b. is recommended as a source of ideas.

SECTION VI - CONCLUSIONS (U)

33. (U) Approach: All conclusions should be aimed at establishing the operation's COMSEC posture relative to the known, suspected, or potential enemy threat. Determinations must be made regarding which communications are susceptible to exploitation and, if possible, which ones are actually being exploited. Before making judgments, the survey team should ensure that all aspects of the problem are fully understood and have been thoroughly considered.

34. (U) Objectives:

a. (U) Three fundamental points must be determined before corrective action recommendations can be formulated. These are: (1) whether or not COMSEC weaknesses exist; (2) the scope and technical aspects of the problem areas identified; and, (3) the seriousness of each problem area in terms of how valuable the intelligence information would be to an enemy should the COMSEC weakness actually be exploited.

b. (U) Once COMSEC discrepancies have been identified and their technical nature determined, the "seriousness factor" must then be assessed. It is true that the technical aspect of the problem normally plays the largest part in determining the overall effort and cost required to correct a specific COMSEC problem. However, it is the seriousness of the problem and its impact on national security that normally dictates the speed with which recommended solutions are implemented. This is why the relative seriousness factor must be determined, even though the full consequences of the problem may never be realized. When considering the damaging effects of a COMSEC weakness in the absence of hard evidence of enemy exploitation, a situation should be considered serious if the enemy's potential for exploiting classified or sensitive information is deemed very good. The weakness will, of course, become even more serious if the content of the communications involved is extremely sensitive.

c. (U) If conclusions do not produce a base from which realistic recommendations can be advanced, it may then be necessary to reexamine certain aspects of the communications, operations, COMSEC, and intelligence data bases and to reorient the analysis process to include refiguring the assigned weights in Matrices 1-4 in Annex A. During a reexamination, some past findings may be invalidated, while others may be reconfirmed. Every effort should be made to avoid uncertain conclusions. Experience has shown that recommendations stemming from such conclusions may be either rejected outright or implemented very slowly.

SECTION VII - RECOMMENDATIONS (U)

35. (U) Solution Criteria. In addition to those considerations discussed in the foregoing Conclusion section, there are a number of other factors which must be considered before arriving at a solution to each COMSEC problem. Some of the more important considerations having a bearing on the solution are:

a. (U) Feasibility of implementing the preferred solution.

b. (U) Technical capability of the organization to implement and successfully employ those measures called for in the solution.

c. (U) Availablility of COMSEC material or resources called for in the recommendation, such as a particular COMSEC hardware system.

d. (U) Criticality of time factor; that is, is the seriousness of the problem such that the solution should be accorded a high priority.

e. (U) Adverse effects the solution may have on other aspects of the operation.

36. (U) Alternate Solutions: Some of the above factors can be determined with a minimum of effort, while others may require more extensive research, especially if a new COMSEC system is being considered as the preferred solution. Survey teams should never lose sight of the fact that it is the supported activity that must accept and implement any proposed recommendations. Consequently, the recommendations should be geared to the capability of the activity to implement them within a reasonable time frame. Where preferred solutions cannot be implemented because of some operational limitation or other factor, alternate or next-best solutions must be advanced. For instance, if secure voice equipments are not available, a suitable operations code may be recommended for use on a tactical voice circuit. This ensures a degree of security that, although less than that provided by secure equipment, is far superior to unencoded plain-language communications.

NOTE: If next-best solutions are decided upon, a useful purpose can still be served by advancing the preferred solution, along with the alternate one. This provides COMSEC requirements personnel with current COMSEC thinking regarding ideal COMSEC solutions and, by doing so, may stimulate future COMSEC system procurement programs within an operation that otherwise might not occur.

37. (U) Recommendation Options:

a. (U) A COMSEC survey may produce a wide range of recommendations, not all of which are directed at solving a particular COMSEC problem. Some can be general in nature and may be offered solely on the premise that a general lack of COMSEC training and indoctrination seemed to prevail within a certain operation. This point is made even though the team should strive for conclusive positions regarding specific COMSEC weaknesses and recommended corrective actions.

b. (U) Most improvement options available to survey teams fall into one of the four broad categories below. Survey teams may recommend:

(1) New COMSEC systems be employed or changes be made to existing ones.

(2) Changes be made to communications procedures (to include limiting communications), transmission security techniques, physical security approaches, classified material control procedures, emission security, and COMSEC practices in general.

(3) Increasing the emphasis on COMSEC training and indoctrination relative to the nature of the hostile threat.

(4) Instituting a program for reviewing the results of past COMSEC recommendations to ensure continuing improvement in the overall COMSEC posture of the operation's communications.

SECTION VIII - SURVEY REPORT (U)

38. (U) Report Format: A written report constitutes the final step of the COMSEC survey. This report notifies the supported activity of the results of the survey including recommendations for improving the COMSEC posture of the operation. The report should be as brief as possible, but contain sufficient information to allow the operational chief(s) to take quick, positive action on the team's recommendations. In all cases, the report should be written with the supported activity in mind and should avoid terms or jargon not readily understood by that organization.

39. (U) Reporting Time Frame: Since the report is the primary means of formally notifying the operational chief(s) of the state of COMSEC within his/her operation, it should be prepared and forwarded as soon as possible after completion of the survey. Timely reporting prevents COMSEC discrepancies within the operation from going unrecognized and thus continuing unattended. When COMSEC weaknesses are deemed too serious to await the final report, a message report should be immediately dispatched to the chief of the operation. As in the case of the final report, the message report should contain sufficient information to allow the operational chief to take quick action to correct the weakness.

40. (U) Report Outline and Content: As a minimum, each final report should contain sufficient information on the following topics:

a. (U) Tasking:

(1) Authority(s) responsible for requesting, authorizing, and planing the survey.

(2) Purpose and scope of survey.

(3) Team Composition.

(4) Type of operation surveyed and activities visited.

b. (U) Survey Findings and Conclusions:

(1) List all COMSEC weaknesses within the operation having a bearing on the vulnerability of the communications to interception, traffic analysis, signal analysis, cryptanalysis, emitter identification, direction finding, imitative communications deception, intrusion, meaconing, jamming, HUMINT pentration and, when known, TEMPEST hazards.

(2) List all COMSEC protection being afforded the operation, including physical security measures. Note secure systems being used and those available, but not being used.

(3) Mention type, volume, and sensitivity of all exploitable plain-language communications being transmitted. Give examples of any EEFIs being divulged.

(4) Comment on overall adequacy of COMSEC guidance contained in the various OPORDS, OPLANS, test plans, COMSEC annexes, SOPs, etc.

c. (U) Recommendations:

(1) Provide solutions for correcting specific COMSEC problems.

(2) Identify problem areas requiring additional study.

(3) Recommend additional training for communications and COMSEC personnel when, in the opinion of the survey team, such training would enhance the overall COMSEC posture of the operation.

(4) Make note of any on-the-spot recommendations made by the team and any follow-up corrective actions being taken by operational personnel.

41. (U) Principles of Report Writing:

a. (U) How well the final report is written has a tremendous bearing on whether the team's recommendations are accepted and acted upon by the supported activity. A poorly written report reflects adversely on the team's efforts and tends to cloud the survey results. To prevent this from occurring and jeopardizing what might otherwise be a very successful survey, written reports should adhere to three basic principles:

(1) Make them clear, concise, and void of ambiguous or unrelated information.

(2) State the conclusions and recommendations in positive terms.

(3) Always provide ample supporting information.

b. (U) Adherence to these principles will not only assure the successful conclusion of COMSEC surveys, but will go far in promoting COMSEC surveys as being the best possible means of improving COMSEC within the Departments and Agencies of the Federal Government.

ANNEX A

COLLECTED DATA ARRAY (U)

1. (U) There are a series of steps for arraying the collected data which should be followed to facilitate a structured analytical approach. These steps are:

a. (U) List each communications-electronics (C-E) system and pertinent characteristics having a bearing on the COMSEC of the operation, such as system purpose, users, transmission mode and media, COMSEC features employed, etc. This listing was called for in paragraph 25. of the basic document.

b. ~~(C)~~ Assess the value of the intelligence information being communicated by any C-E system listed in step a., above, or possibly being divulged/exploited through any unsound physical security practice within the operation. Some of the more sensitive types of information and materials include:

(1) Nuclear forces/weapons command and control (C^2).

(2) Strategic C^2 involving National Command Authority, CINCS, etc.

(3) Presidential.

(4) Foreign intelligence.

(5) Diplomatic.

(6) Space systems and technology.

(7) Tactical weapons/combat C^2.

(8) Administrative/logistics support.

(9) National economic, RDT&E, defense contractor related, etc.

(10) Identification features.

(11) COMSEC materials, e.g., keying material, OPCODES, and crypto-equipments.

Matrix 1 in this annex provides a method of weighing the intelligence value of each type of information in relation to its C-E and/or physical security source.

c. (U) Assess the vulnerability of each C-E system and physical security source to various hostile exploitation attacks. Depending upon the operation, it may be necessary to make the assessment

CLASSIFIED BY NSA/CSSM 123-2
REVIEW ON 3 July 2000

for both a peacetime and wartime environment, since the threat may be substantially different for each situation. (This would hold true for steps d.-f., below, as well.) Matrix 2 shows one type of recommended vulnerability assessment scheme.

d. (U) Postulate adversary's intent to exploit particular vulnerabilities via traffic analysis, cryptanalysis, signals analysis, jamming, HUMINT penetration, etc. Matrix 3 provides a method of showing intent to exploit.

e. (U). Speculate on the adversary's successes should an attempt be made to exploit one or more of the vulnerabilities cited. In addition to the vulnerabilities themselves, the risk of the hostile collector being detected and overall costs are other factors in determining his success ratio. Matrix 4 shows one method of depicting exploitation successes.

f. (U) After sequentially filling in Matrices 1-4, formulate COMSEC strategy to counter the hostile threats to all assessed C-E/COMSEC vulnerabilities. This strategy has to take into account life-cycle costs of implementing the COMSEC measure, manpower and other operational resources required, and any adverse effects the COMSEC measure may have on other aspects of the operation.

2. ~~(C)~~ COMSEC strategy for enhancing the COMSEC posture of an operation is dictated by the assigned weights in Matrices 1-4. For example, if the "intelligence value" of a given source in Matrix 1 is in the 6-10 range, and the "exploitation success" of a hostile attack (e.g., traffic analysis) against that same source in Matrix 4 ranges between 3-10, then COMSEC improvement should be deemed mandatory. (Vulnerability figures in Matrix 2 will normally be equal to or higher than "exploitation success" figures in Matrix 4.) In the above example, should the "intelligence value" range between 6-10 and the "exploitation success" figure range between 1-2, then COMSEC improvement should be considered desirable (but not necessarily mandatory). "Intelligence value" between 3-5 and "exploitation success" between 1-2 would indicate COMSEC improvement is probably not required. In order to arrive at a "no COMSEC improvement required" assessment, "intelligence value" would have to be 0-10 and "exploitation success" 0, or "intelligence value" 0 and "exploitation success" 0-10.

3. ~~(C)~~ "System vulnerability" in Matrix 2 is the key factor in determining "exploitation success" in Matrix 4. Therefore, the overall COMSEC strategy should be geared to lowering the numerical values (hopefully to "0") of any cited vulnerability in Matrix 2, which should then have a corresponding lowering effect on the "exploitation success" figures in Matrix 4. (This is so, even though "intelligence value" in Matrix 1 and "intent to exploit" in Matrix 3 may still remain high.) An example of such an assessment would be nuclear weapons intelligence being transmitted over a very secure cryptographic system, where the intelligence value would be high, the most critical vulnerability "0" (i.e., content not

exploitable), the intent to exploit high, and exploitation success via cryptanalysis "0". It can be seen, therefore, that many combinations can be derived from use of the four Matrices, which is exactly what they are designed to reflect.

4. (U) HUMINT penetration will be the primary hostile attack against physical security sources listed in the four Matrices. The general "rule-of-thumb" scale used in paragraph 2., above, is also applicable to physical security sources when considering COMSEC strategy for correcting assessed vulnerabilities. That is, if the value of the intelligence information (keying material, OPCODES, crypto-equipments, etc.) being processed by a COMSEC material storage or destruction facility is rated between 6-10 in Matrix 1 and the HUMINT exploitation success figures against these sources in Matrix 4 range between 3-10, then COMSEC improvement should be considered mandatory. It requires a little more imagination to use this "rule-of-thumb" scale when the source is a COMSEC accounting system, due to the lack of physical material (except the accounting records themselves) in which to exploit. However, because COMSEC accounting system weaknesses can aid hostile exploitation of other physical security sources without risk of detection, an attempt should be made to use the above "rule-of-thumb" scale when assessing COMSEC accounting systems.

5. (U) Because of the subjective nature of performing most COMSEC survey analytical work, there are few hard-and-fast rules for survey teams to follow. This brings into play the talent and experience of the COMSEC analyst, whose task it is to ponder a multitude of factors in order to arrive at proper conclusions and, ultimately, recommend appropriate solutions to COMSEC problems. The procedures and Matrices in this Annex, when used in conjunction with the analytical questions in Annexes B-E, are excellent aids in helping COMSEC analysts to better perform their task.

~~CONFIDENTIAL~~

SCALE = 0-10

10 = Critically important
8-9 = Very important
6-7 = Considerable importance
3-5 = Some value
1-2 = Questionable value
0 = None

MATRIX # I - INTELLIGENCE VALUE

	Intelligence Information →	Nuclear weapons	Strategic C2	Presidential	Foreign intelligence	Diplomatic	Space related	Tactical C2/weapons	Administrative	Logistics support	Economic info.	RDT&E info.	Contractor related	Identification	COMSEC Material
Communications-Electronics Sources	Data System A														
	Data System B														
	Voice System A														
	Voice System B														
	TTY System														
	CW System														
	Facsimile System														
	Telemetry System														
	IFF/SIF System														
Physical Security Sources	COMSEC Material Storage Facilities														
	Shipping/Receiving														
	Accounting System														
	Destruction Facilities														
	Communications Facilities														

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

A5

SCALE = 0-10

10 = Extremely vulnerable
8-9 = Very vulnerable
6-7 = Moderately vulnerable
3-5 = Slightly vulnerable
1-2 = Almost none
0 = None

MATRIX # 2 - SYSTEM VULNERABILITY

Hostile Attacks --->

		Interception	Traffic Analysis	Signals Analysis	Cryptanalysis	Direction Finding	Jamming	Intrusion	Spoofing	Emitter ID	HUMINT Penetration	TEMPEST Exploitation	Imitative Communication Deception
Communications-Electronics Sources	Data System A												
	Data System B												
	Voice System A												
	Voice System B												
	TTY System												
	CW System												
	Facsimile System												
	Telemetry System												
	IFF/SIF System												
Physical Security Sources	COMSEC Material Storage Facilities												
	Shipping/Receiving												
	Accounting System												
	Destruction Facilities												
	Communications Facilities												

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

SCALE = 0-10

10	Certain
8-9	Probable
6-7	Limited
3-5	Possible
1-2	Very doubtful
0	No intent

MATRIX # 3 - INTENT TO EXPLOIT

	Hostile Attacks →	Interception	Traffic Analysis	Signals Analysis	Cryptanalysis	Direction Finding	Jamming	Intrusion	Spoofing	Emitter ID	HUMINT Penetration	TEMPEST Exploitation	Imitative Communication Deception	
Communications-Electronics Sources	Data System A													
	Data System B													
	Voice System A													
	Voice System B													
	TTY System													
	CW System													
	Facsimile System													
	Telemetry System													
	IFF/SIF System													
Physical Security Sources	COMSEC Material Storage Facilities													
	Shipping/Receiving													
	Accounting System													
	Destruction Facilities													
	Communications Facilities													

~~CONFIDENTIAL~~

CONFIDENTIAL

SCALE = 0-10

MATRIX # 4 - EXPLOITATION SUCCESS

10	Total success
8-9	Highly successful
6-7	Moderately successful
3-5	Limited success
1-2	Very little success
0	None

	Hostile Attacks →	Interception	Traffic Analysis	Signals Analysis	Cryptanalysis	Direction Finding	Jamming	Intrusion	Spoofing	Emitter ID	HUMINT Penetration	TEMPEST Exploitation	Imitative Communication Deception	
Communications-Electronics Sources	Data System A													
	Data System B													
	Voice System A													
	Voice System B													
	TTY System													
	CW System													
	Facsimile System													
	Telemetry System													
	IFF/SIF System													
Physical Security Sources	COMSEC Material Storage Facilities													
	Shipping/Receiving													
	Accounting System													
	Destruction Facilities													
	Communications Facilities													

CONFIDENTIAL

ANNEX B

TRANSMISSION SECURITY ANALYTICAL QUESTIONS (U)

1. Were any transmissions unnecessary to the functional needs of the operation?

2. Were messages lengths and transmission times reduced to the minimum?

3. Was operator chatter prevalent?

4. Was an excessive number of radio checks held?

5. Would an enemy's direction-finding efforts be reasonably successful against the bulk of the transmissions?

6. Due to their nature, could most of the transmissions be easily intercepted? If so, why? (Excessive power output? Low frequency? Antenna system propagation pattern? Type of transmission?)

7. Could any interceptable transmissions be attributed to poor circuit discipline or nonadherence to proper procedures?

8. Were security indiscretions frequently observed? Did most occur over plain-language radiotelephone circuits?

9. Were most violations caused by exessive operator chatter?

10. Would any transmission signals definitely extend into enemy territory? If so, could the offending transmission(s) be made via another method or circuit to prevent this from occurring?

11. Were call signs, suffixes, and frequencies static or changing?

12. Would the method of assigning and using call signs allow hostile intercept operators to predict call sign changes and thus maintain target continuity?

13. Were international call signs often used?

14. Were call signs and frequencies both changed at the same time?

15. Were collective call signs used to the maximum extent possible?

16. Would the call sign suffixes greatly aid an enemy traffic analyst in determining the level of command, order-of-battle, and net structure?

~~INDIVIDUAL PARAGRAPHS ARE UNCLASSIFIED, HOWEVER, THE COMPILATION OF INFORMATION IS CONFIDENTIAL~~

CLASSIFIED BY NSA/CSSM 123-2
REVIEW ON 3 July 2000

17. Are specific frequencies used repeatedly for certain operations or functions?

18. Is the frequency population too limited to accommodate periodic changes?

19. Were plain-language radio nets or unsecure conventional telephone circuits being used to conduct sensitive operations? How perishable is the information being passed over these systems?

20. Were any protected wireline or fiber optic distribution systems available to the operation and are they located entirely within the confines of the operational spaces? Are these circuits being used to transmit classified information of a higher classification than authorized?

21. Were the protective distribution systems established in accordance with ACP 122 instructions? If not, what guidance was used?

22. Do any unprotected telephone circuits contain microwave or sideband transmission links?

23. Were any unprotected circuits being used to establish secure, on-line circuits? How much information about the net structure and order-of-battle was being divulged through this practice?

24. Did any communications procedural errors reveal any valuable intelligence information?

25. Did net control stations maintain adequate control of their nets?

26. Did net control stations use a standard procedure for challenging outstations that committed a security violation?

27. Were radio checks always made just prior to the start of an operation, thus serving as alerting indicators? Are the radio checks divulging such things as the number, type, and location of the participating units?

28. Conversely, is radio silence always enforced just prior to commencing a certain operation, thereby also serving as a source of tip-off?

29. Were any other cases of enforced radio silence noted that might serve as an indicator that some action by the operation was imminent?

30. Are any nets/circuits activated on a predictable schedule?

31. Are any reports transmitted on a regular, predictable schedule? Assuming interception, what intelligence information could be derived from regularly transmitted reports?

32. Do certain activities normally take place immediately following particular transmissions? Would this correlation be readily apparent to an enemy, thus allowing him to predict forthcoming events?

33. Did any unclassified, plaintext messages ever reference a secure, classified message? Were any classified messages ever canceled by an unclassified message?

34. Were messages being properly formatted?

35. Are any message formats stereotyped as to form, length, address groups, and precedence? Is there a difference between practice message formats and operational message formats?

36. Do the practice messages contain exploitable information of intelligence value?

37. Based on all information reviewed, would the operation's communications be considered vulnerable to traffic analysis, signals analysis, or emitter identification?

38. How liable to imitative deception would the communications be?

39. Has the operation instituted any significant transmission security improvement programs recently? Are any improvement programs in the planning stage that will correct a number of COMSEC discrepancies noted within the operation?

40. What do the communications personnel regard as the most serious transmission security problem facing the operation?

41. Is authentication properly used when it is required?

ANNEX C

CRYPTOGRAPHIC SECURITY ANALYTICAL QUESTIONS (U)

1. Were secure, on-line crypto-equipments available in sufficient numbers, but not fully used? Did any nonuse stem from lack of compatible keying material or other related COMSEC material? Was any nonuse due to lack of trained operators or maintenance personnel?

2. Were all equipments being properly operated and entirely in the secure mode?

3. Was crypto-equipment compatibility a major problem?

4. Was sufficient keying material available to resupply all net members in the advent of a keying material compromise?

5. Were keying material changes made in accordance with prescribed cryptoperiods?

6. Were messages prepared in accordance with approved formats?

7. When called for, were CODRESS procedures fully understood and followed?

8. Were any manual systems being used to encode/encipher special communications that normally require encryption by a high-grade machine system?

9. Did each controlling authority issue specific instructions regarding which cryptosystem should be used for each type of message transmitted?

10. Did communicators show an awareness of the need to authenticate and when to authenticate? When observed, was authentication successfully and properly accomplished?

11. Did operators seem knowledgeable of what constitutes a cryptocompromise? Were procedures for reporting cryptoviolations and possible compromises posted in all cryptocenters?

12. Were unauthorized "homemade" operations codes being used to transmit classified information?

13. How suitable are the authorized codes? Would a change in vocabulary or format bring about an increase in their use?

14. Are common operations codes held by all participating units having a need to communicate securely?

~~INDIVIDUAL PARAGRAPHS ARE UNCLASSIFIED; HOWEVER, THE COMPILATION OF INFORMATION IS CONFIDENTIAL~~

CLASSIFIED BY NSA/CSSM 123-2
REVIEW ON 3 July 2000

15. Are any authorized codes being misused, such as excessive use of an operations code to encode "pro forma" messages?

16. Is plain text being mixed with encoded messages when not authorized, thereby weakening the security of the encoded portions?

17. Are brevity codes being used to encode classified messages in the belief that they provide security?

18. Is the lack of secure voice equipments the major COMSEC weakness?

19. Are any secure voice nets/circuits in the planning stage?

20. Could any COMSEC problems be attributed directly to a lack of COMSEC requirements planning?

21. Were COMSEC aids being received in a timely manner?

22. Did those personnel charged with fulfilling COMSEC requirements seem sufficiently knowledgeable of the latest COMSEC systems available and the proper procedure for obtaining such systems?

23. Are crypto-equipment alarm checks made at prescribed times?

24. Are crypto-equipment operating instructions available to all operators who require them?

25. Have there been any recent instances when the prescribed cryptoperiod for cryptographic keying material have been exceeded?

26. Are crypto-equipment maintenance services adequate to ensure continuity of secure communications?

27. If cryptographic keying variables are generated locally, are they effectively and securely managed?

ANNEX D

PHYSICAL SECURITY ANALYTICAL QUESTIONS (U)

1. Are all communications facilities properly constructed and located in secure, well controlled areas? Are they fixed, mobile, or a combination?

2. Can classified conversations be heard by unauthorized persons outside these spaces because of inadequate soundproofing or location of the spaces?

3. Is the "need-to-know" principle adhered to regarding access to all communications facilities? Are the facilities properly secured when unoccupied?

4. Is a list maintained of all persons authorized to enter each cryptocenter? Are "RESTRICTED AREAS" properly identified and plainly marked?

5. Are all COMSEC materials being properly received, stored, and accounted for?

6. Do custodians and users take inventory often enough to prevent lost or missing material from going undetected for excessive periods of time?

7. Are COMSEC materials afforded proper security protection during transportation? Are the couriers employed to transport COMSEC materials locally properly cleared?

8. Are destruction facilities adequate for destroying COMSEC material that is routinely superseded?

9. Are the destruction methods safe to use and the procedures easy to follow?

10. Are the COMSEC material emergency destruction facilities and techniques adequate?

11. Overall, are physical security directives and regulations being adhered to?

12. Are protected distribution systems properly installed and are they inspected and patrolled in the prescribed manner?

~~INDIVIDUAL PARAGRAPHS ARE UNCLASSIFIED; HOWEVER, THE COMPILATION OF INFORMATION IS CONFIDENTIAL~~

CLASSIFIED BY NSA/CSSM 123-2
REVIEW ON 3 July 2000

ANNEX E

GENERAL COMSEC ANALYTICAL QUESTIONS (U)

1. Do the OPORDS, OPLANS, SOPs, and COMSEC annexes provide realistic COMSEC guidance? Do the OPLANS, SOPs etc., call for notifying the operational chief of detected COMSEC insecurities?

2. Is COMSEC planning effective? Is COMSEC effectively managed?

3. Did the COMSEC measures address the various phases of the operation and provide for a changing communications environment? Were COMSEC objectives achieved?

4. Do communicators and COMSEC personnel exhibit an awareness of the vulnerabilities associated with each communications system?

5. Are the meanings of the code words, nicknames, and certain functional aspects of the operation referred to indirectly over unsecure circuits during the planning, execution, and postevaluation phase of the operation? If so, would such indirect references be sufficient to allow an enemy to determine the scope of the operation and possibly predict future U.S. intentions?

6. Is COMSEC training adequate among communications personnel?

7. What type of operator training would best correct the kinds of procedural errors noted?

8. Is the threat to U.S. communications being properly emphasized within the operation?

9. Of those persons interviewed, what did most regard as the major COMSEC problem(s) facing the operation?

10. Generally, what was the view of operational personnel regarding the availability, usability, and security of the COMSEC systems being employed?

11. If operators/users are not satisfied with the performance of some cryptosystems employed, how does this problem impact on the COMSEC posture of the operation?

12. Are crypto-equipments available in the needed types and quantities to meet operational requirements?

~~INDIVIDUAL PARAGRAPHS ARE UNCLASSIFIED, HOWEVER, THE COMPILATION OF INFORMATION IS CONFIDENTIAL~~

CLASSIFIED BY NSA/CSSM 123-2
REVIEW ON 3 July 2000

ANNEX F

INDEX OF NACSEMs/NACSIMs PUBLISHED TO DATE

NACSEM/NACSIM NO.	TITLE	DATE
2001	Contingency Program for COMSEC Aids	27 Aug 75
2002	COMSEC Nomenclature Systems	2 Oct 75
4002	Fundamentals of Signals Security	Jul 75
4004	National COMSEC Information Memorandum (NACSIM), COMSEC Survey Guide	Jul 80
5100	Compromising Emanations Laboratory Test Standard, Electromagnetics	Mar 74
5101	Technical Rationale for Compromising Emanations Laboratory Test Standards, Electromagnetics	Oct 70
5102	Administrative Guidelines for Compromising Emanations Laboratory Test Standards, Electromagnetics	Oct 70
5103	Compromising Emanations Laboratory Test Standard, Acoustics	Oct 70
5104	Technical Rationale for Compromising Emanations Laboratory Test Standard, Acoustics	Oct 70
5105	Administrative Guidelines for Compromising Emanations Laboratory Test Standard, Acoustics	Oct 70
5106	Compromising Emanations Analysis Handbook	Dec 71
5108	Standardize Receiver/Amplifier Evaluation Procedures	Jul 74
5109	TEMPEST Testing Fundamentals	Mar 73
5110	Facility Evaluation Criteria - TEMPEST	Jul 73
5112	NONSTOP Evaluation Techniques	Apr 75
5201	TEMPEST Guidelines for Equipment/System Design	Sep 78
5204	Shielded Enclosures	May 78

NACSEM/NACSIM NO.	TITLE	DATE
7001	COMSEC Planning Guide for Manual Cryptosystems	Oct 74
7002	COMSEC guidance for ADP Systems	Sep 75

INDEX OF NACSIs PUBLISHED TO DATE

NACSI NO.	TITLE	DATE
1001	Management of the National COMSEC and EMSEC Issuance System for NACSIs and NACSEMs	5 Jan 72
2001	Program for the Management and Utilization of Excess Communications Security Material	8 Jun 70
2002	Keying Material Management	8 Aug 72
2005	Communications Security (COMSEC) Systems and Equipment Modification	Jun 74
2007	Standard Criteria for Controlling COMSEC Equipment Loans	11 Nov 77
4000	Guidelines for the Conduct of Communications Security Survey Activities	3 Jan 80
4002	KY-8 Wireline Usage	23 Sep 77
4003	Classification Guidelines for COMSEC Information	1 Dec 78
4004	Controlling Authorities for COMSEC Keying Material	8 Sep 78
4005	Safeguarding and Control of Communications Security Material	12 Oct 79
4007	Management of Manual Cryptosystems	27 Jul 76
7001	Cryptographic Equipment Maintenance and Training	12 Apr 72
8101	Operational Doctrine for PARKHILL	Jan 79
8102	Operational Doctrine for VINSON and BANCROFT	Feb 79