

902d MI Group Pamphlet 381~3

DEPARTMENT OF THE ARMY Headquarters, 902d Military Intelligence Group Fort George G. Meade, Maryland 20755

902d MI Group Pamphlet No. 381-3

22 April 1976

Military Intelligence DIRECT SUPPORT COMPREHENSIVE COUNTERINTELLIGENCE PROGRAM (DSCCP) (U)

- REFERENCES: See APPENDIX A.
- (U) PURPOSE: This pamphlet establishes policy, guidance, and standardized procedures for the conduct of all-source, multi-discipline counterintelligence support within the 902d MI Group's area of operation.

(U) GENERAL:

- The Commander, 902d MI Group, has the responsibility to notify commanders of Army installations and units in the group's area of operation
- (1) Any situation or condition exists that poses a threat to the internal security of that Army element.
- (2) Any situation exists that might adversely affect the commander's capability to perform his mission.
- (3) Information indicates a probable employement of military resources to counter a threat to the installation.

In order to acquire information of situations or conditions that may pose a threat to the supported commander, field elements must aggressively seek it and not wait for it to be reported through normal sequence of events. This is particularly essential for those units/installations declared to be critical sensitive.

The DSCCP is one of a series of graduated intensity counterintelligence programs designed to provide the proper coverage based on the security vulnerability of a particular installation. In relationship to other graduated counterintelligence programs listed in USAINTA Regulation 381-100, the DSCCP would, in certain instances, serve as a means of identifying the need for programs of greater intensity such as SVAs, or SAVEs, or, in other instances, may serve as follow-up support subsequent to such intensified services. It provides the broad spectrum of coverage to include a multidiscipline approach with provisions that the information gathered be reported expeditiously to the responsible commander. The program systematically focuses on providing threat information on the most critical area within the target installation in order to provide the required information to the supported commander. CLASSIFEED BY: COR USALN'TH

REGRADED UNCLASSIFIED SEP -5 1997 ON BY CDR USAINSCOM FOI/PO

AUTH PARA 1-603.DoD \$200-1-R

EXEMPT FIRST 6. DE 17 PERMISSIPEGACION

3 DECEMBER 2004

<u>.</u>.

902d MI Group Pamphlet No. 381-3

22 April 1976

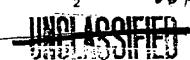
This program is not synonymous with, nor is it identifiable with, the Internal Counterintelligence Program, Special Operations as defined in FM 30-17A, or the Special Covert Operational Personnel Insertion (SCOPI) as defined in USAINTA Regulation 381-100.

(U) CONCEPT:

- The Direct Support Comprehensive Counterintelligence Program (DSCCP) is an overt, dedicated counterintelligence Security support program with the objective of detecting or anticipating situations and factors from any source (HEMINT/SIGIRT/PHOTINT) which are or may become detrimental to the security posture of the supported installation. It plays a Direct Support Special Agent (DSSA) in an overt continuous als of acquiring information and providing it to the commander in a timely manner, while concurrently providing sound recommendations for the reduction and/or elimination of security hazards, vulnerabilities on threats posed by hostile factors.
- b. The DSSA obtains the required information from overt investigative activities and from a number and variety of sources and contacts within and in the vicinity of the supported installation. Confidential sources are not utilized. He is fully supported in this task by the intervening echelons at Field Offices, Group, and USAINTA.
- c. The DSCCP is a complementary service provided to the supported commander to assist him in improving the security posture of his installation. It is not intended to duplicate nor to usurp the functions and responsibilities of the G-2 or of the Security Manager.

5. (U) RESPONSIBILITIES:

- a. The Commander, 902d MI Group, is the approving authority for all DSCCP operations conducted within the group's area of operation.
 - b. The S3, 902d MI Group is responsible for the following:
- (1) Coordinating the selection of units/installations as candidates for DSCCP with the appropriate USAINTA staff elements.
- (2) Monitoring DSCCP operations on a continuing basis and periodically informing appropriate USAINTA staff elements of their progress.
- ...(3) Conducting an annual review of each DSCCP operation to determine if it is still necessary and if so, to asure that it remains viable.
 - c. Pield Office Commanders are responsible for the following:
- (1) Initiating proposed DSCCP operations for installations located within their areas of operation.



22 April 1976

902d MI Group Pamphlet No. 381-3

. .

. 1

-

- (2) Conducting DSCCP operations within their area after approval by the Group Commander and coordination with the supported commanders.
- (3) Designating the DSSA for each DSCCP operation, providing followup support, and arranging for DSSA clearance and access to compartmented information as required.
- (4) Briefing of the supported commanders on the results of DSCCP operation at regular intervals per mutual agreements.
- (5) Establish procedures to maintain continuity of the program during absences of the DSSA. When possible, an alternate DSSA will be assigned: 🏬

PROCEDURES AND SCOPE:

- The designation of installations or Army elements as candidates for the DSCCP will be a coordinated action between the Field Office Commander and the supported commander. In some cases, the action may be directed by the Group Commander or USAINTA following a request for special counterintelligence support from a major commander. Regardless of the origin of the request, DSCCP operations will always be conducted with the full consent and knowledge of the supported commander.
- The selection of installations to be considered for the DSCCP must be discriminatory and based on a genuine need for this manpower intensive service in order to avoid over-commitment of assets. The target installation must be one that is on the ACSI Sensitive Installation and Unit List (SIUL) and one that is a potential or actual target of hostile intelligence services. It is recognized that some field offices and resident offices have numerous sensitive installations in their area, many of which may be categorized as critical. Therefore, it is essential that each FO/RO maintain a listing of these installations in order of priority. In determining the order of priority, factors such as mission sensitivity, and impact of compromise on the security of the United States, etc., will all have to be analyzed and a value judgement must be made based upon actual knowledge of the local conditions, as to which installation has a greater need for special The installations heading the list will get first consideration.
- Proposed concept will be submitted to the Group Commander by letter for approval. The letter will indicate the installation commander's concurrence in the program. The concept will contain a listing of missions, sensitivities, and those internal and external factors which may pose a threat to the installation. Vulnerabilities to human sources,

ON SFP -5 1997 BY CDR USAINSCOM FOUPO AUTH PARA 1-603 DoD \$200.1-R

902d MI Group Pamphlet No. 381-3

1 may 12 8791

22 April 1976

مأجار

communications intercept, overhead and ground photography, and other appropriate technical/scientific factors will be included if known. This information will be extracted from the target analysis (Para 7a) or from the SVA if one has been completed. The concept must address actions to be taken to detect and counter these threats.

- d. (U) Occasional expenditures of ICF in support of this program is authorized and will be processed in compliance with the provisions of AR 381-141 and USAINTA Regulation 381-1. Recurring expenditures will be supported by a formal request for authority if such expenditures are anticipated.
- concerning persons and organizations not affiliated with the Department of Defense are prohibited unless authorized under the provisions of AR 180-13.

7(U) GUIDELINES:

The actions listed below are considered to be minimum essential for the implementation of this program and are not to be considered as all-encompassing. They should be modified as appropriate to meet situations and needs peculiar to the supported installation. Common sense and experience will likely dictate additional or supplementary means to be employed in order to successfully attain the objective.

- a. (U) Conduct a target analysis of the unit/installation to identify, in order of priority, the most critical and vulnerable areas and the multi-discipline threats to which they are exposed. Reference will be made to the following: USAINTA Security Support Bulletins, "THREAT" Manuals, completed SVA/SAVE Reports, CI Survey and Inspection Reports, PM/MP Crime Statistics and Incident Reports, and Communications Security Reports, when available and applicable. The original copy of the analysis will be maintained at the PO/RO level. Appropriate data will be extracted and included in the initial Quarterly Progress Report. The analysis should be reviewed and updated periodically in subsequent Quarterly Progress Reports.
- b. (U) Assign a mature, experienced MI Special Agent as a Direct Support Special Agent (DSSA) to provide all-source direct support to the supported commander or his designated representative. The DSSA must become intimately knowledgeable of the supported command's mission, functions, security status and vulnerabilities. As the program will be overt in nature, the DSSA will be known as the primary USAINTA point of contact to all within the supported units/installations. The DSSA will require a TOP SECRET clearance and an SI/SAO special access.

REGRADED UNCLASSIFIED ON SEP -5 1997. BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DoD \$200.1-R -CONFIDENTIAL

c. The task of the DSSA is to develop a sufficient number of sources of information to provide the best possible coverage to the unit/installation and personnel of the element to detect security vulnerabilities, and make sound recommendations for their reduction and/or elimination. The DSSA should work closely with the security manager to coordinate appropriate matters and to avoid duplication of effort. However, care should be taken not to duplicate or usurp functions and responsibilities rightfully assigned to the security manager.

- (1) Human sources of information will include Conventional Sources (Incidental, Casual, and Official) and Liaison Contacts as described in Chapter 6, FM 30-17. Confidential Human Sources will not be utilized. Anonymity may be provided through the provisions of the Privacy Act of 1974 when the source so requests. The association between the DSSA and Conventional Sources or Liaison Contacts will not normally be classified.
- (2) Maximum use will also be made of Documentary and Technical/Materiel Sources to include, but not be limited to, SATRAN Messages, Department of the Army intelligence publications and/or bulletins;
 -USAINTA Security Support Bulletins and "THREAT" Manuals; SAVE/SVA reports; Military Police Reports, and Serious Incident Reports. Special attention should be paid to message traffic concerning alerts, advisories or warnings concerning events or situations affecting the supported command.

d. A contact card file will be maintained at the supporting office to identify conventional sources and liaison contacts. This file will be integrated into the existing contact card file already established for use in the routine mission of the FO/RO. It must be readily available for DSSA personnel at all times. Individual cards will be annotated when the contact is in support of a specific DSCCP operation. IACs will be conducted on casual sources with the results reflected in the contact card file.

atic review of the dossiers of personnel occupying key and sensitive positions to insure that all such personnel have been properly cleared and to determine if unresolved security matters exist. This issue will be discussed with the supported commander if such a review is deemed necessary, the DSSA should recommend that the commander undertake the action. If the commander requests that the review be conducted by the DSSA, then the matter will be referred to group headquarters where resolution will be made in conjunction with the appropriate USAINTA staff elements. The DSSA may assist the supported command in the review of dossiers but may not take any investigative action to resolve issues. He will advise the supported command to submit requests to USAINTA whenever investigative action is indicated.

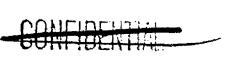
No. 381-3



Reporting of Information:

- To the local commander: Information of counterintelligence interest affecting the security posture of the unit/installation will be reported to the supported commander or his designated representative in a timely and complete manner. The information may be reported orally, by Agent Report format, or by Summary of Information (SOI) format, as appropriate. While most items of information will be passed on an oral basis only, there may be certain instances when the commander will desire written reports from the DSSA to be later attached as backup information to his Request for Investigation. In these instances, ARs containing the adverse allegation may be passed when the full consent of the sources of the information has been obtained. Bowever, when a source of information desires confidentiality, to protect the source, the DSSA can then pass in the information only on an oral basis or by SOI format. Regardless of the manner in which the information was passed to the supported command, a report of the information provided to the supported command will be summarized in the Quarterly Progress Report to this headquarters with an indication of the actions taken by the supported command (see Para 7h below).
- (2) (U) Other: Information of counterintelligence interest to the intelligence community or other agencies will be reported in accordance with established procedures utilizing normal reporting vehicles such as oral reports, Agent Reports, Spot Reports or Summaries of Information as appropriate. Information reports will be classified according to their content. Such reports will indicate when and to whom the information was passed and what action the command has taken or plans to take. Subject blocks, special warning notices and Privacy Act caveats, etc., will be those utilized in established investigative activity procedures. (AR 381-20 and USAINTA Reg 381-100).
- (3) (U) When fragmentary information of counterintelligence interest is initially surfaced, the DSSA will attempt to determine whether or not the information is credible prior to reporting it to the supported Commander. Preliminary checks may be made only to the extent authorized in para 3-6, USAINTA Reg 380-100. Should this prove to be insufficient to establish the credibility of the information, the DSSA will then refer the matter to group headquarters for coordination with USAINTA. Credible information concerning a member of the supported command should be used to support a formal Request for Investigation to USAINTA.
- (4) The supported commander or his designated representative will be orally briefed on all items of threat information concerning his command, or be provided written reports as appropriate. Examples of the types of threat information include satellite overflights, Soviet bloc

REGRADED UNCLASSIFIED
ON
BY CDAFOSANSCOM FOI/PO AUTH PARA 1-603 DOD \$200.1-R



902D MI Group Pamphlet No. 381-3

22 April 1976

country commercial overflights, communications intercept capabilities/
vulnerabilities from air, ground or water, personnel security vulnerabilities and others as listed below. Depending upon the source of the
information and its previous distribution within the intelligence community, the information may be passed laterally or to higher echelons in
accordance with established reporting requirements. All information
gleaned from the operation will be briefly summarized in the Quarterly
Progress Report.

- g. (U) A list of EEI will be developed by the DSSA in order to focus specialized coverage on the specific requirements of the local situation and the supported commander. Examples of EEI are attached at APPENDIX B. It should be noted that the EEI contain items of specific interest to the supported commander and other items that pertain to lead material for use by the US Army intelligence community. A copy of the developed EEI list will be attached to the initial Quarterly Progress Report.
- h. (U) A Quarterly Status Report in the format contained at APPENDIX C will be submitted to Group Headquarters no later than 10 working days following each calendar quarter. The first report will be due after the completion of the first full quarter of operation after initiation. The report should reflect the developments and progress of the operation, problems encountered, information obtained during the reporting period, future actions contemplated and lessons learned or recommendations as appropriate.
- Reducing Vulnerabilities: Once a security weakness or hazard has been identified, the DSSA then has the responsibility to make sound recommendations for corrective actions to be taken by the supported commander to reduce or eliminate them. In making these recommendations, the DSSA must use good judgement based upon his background and experience, cost verses absolute security, knowledge of similar instances, common sense, and an intimate knowledge of those technical and/or specialized security services and/or investigations available to the supported commander from other USAINTA elements. Each corrective action must be viable, made on its own merit, be practical and be within the capability of the supported command. USAINTA Security Support Bulletins contain excellent examples of "quick-fix" solutions. In those rare instances when corrective actions cannot be accomplished due to cost restrictions or limited resources available to the command, the commander must be made aware of, and accept the possible security risk(s) involved.
- 9. It is visualized that situations, incidents or conditions may be uncovered which could have serious deleterious effect on the security

REGRADED UNCLASSIFIED
ON SEP -5 1997_
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD \$200.1-R

869

CONFIDENTIAL

CONFIDENCE:

22 April 1976

REGRADED UNCLASSIFIED

AUTH PARA 1-603 DoD 5200.1-R

posture of the installation and could not be resolved through the techniques of the DSCCP. In these cases, the matter should be expeditiously referred to Group Headquarters where it will be brought to USAINTA's attention for resolution, considering ICIPs, SCOPIs, Special Operations, or other more sophisticated methods.

- 10. (U) The application of the DSCCP to a supported installation is a special effort and will probably require the services of the DSSA on a near full time basis with additional manhours of support furnished by FO and Group Headquarters. Consequently, FO Commanders and RO SAICs should proceed with caution in offering this service to commanders to prevent over-extending their resources. Nevertheless, the DSSA approach of the DSCCP is sound and could well be applied to other installations in the area of operations but to a much lesser degree than in the DSCCP. This should be done as a routine matter and no formal approval is required. Thus, one MI Special Agent could become the DSSA to several installations of lower priority.
- 11. (U) This pamphlet provides policy and guidance for 902d MT Group personnel in the conduct of all-source, multi-discipline counterintelligence support within the area of responsibility of the 902d MT Group. It complements existing US Army Regulations, USAINTA Regulations and USAINTA policy and guidance. Nothing in this pamphlet shall be construed to contravene or to be in conflict with existing US Army or USAINTA policy. In the event that possible conflicts may arise, the provisions of existing US Army and/or USAINTA policy will apply. Any questions pertaining to possible conflict of the provisions of this pamphlet with existing policy will be addressed to this headquarters, ATTN: MIIA-GPB-AC, for further staffing with appropriate USAINTA staff elements. Comments and recommendations are encouraged and should be submitted on DA Form 2028 (Recommended Changes to Publications) to this headquarters for consideration and staffing.

3 Incl

Appendix A - References

Appendix B - EEI

Appendix C - Quarterly Report

HASSEL L. PARK Colonel, MI

Commanding

DISTRIBUTION:

B plus

10-S3, 902d MI Group

1-MIIA-SO

1-DARCOM LNO

1-USASA LNO

1-FORSCOM LNO

1-Cdr, 525th MI Group

1-MIIA-ADM 2-MIIA-CI

Z-MIIM-CI

1-MIIA-IN

1-USACC LNO

1-HSC LNO

1 777777

.1-TRADOC LNO

1-Cdr, 901st MI Det

870

CONFIDENTIAL

APPENDIX A TO 902D MI GROUP PAMPHLET 381-3

REFERENCES

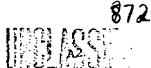
1. Army Regulations:

- a. AR 18-7, Army Information and Data Systems, Data Processing Installation Management, Procedures, and Standards.
 - b. AR 190-13, the Army Physical Security Program
 - c. AR 340-21, Office Management, The Army Privacy Program.
- 5200.1-R (DODISPR).
- e. (C) AR 380-10, Department of the Army Policy for Disclosure of Military Information to Foreign Governments (U).
- f. AR 380-13, Security, Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations.
 - g. AR 380-150, Access to and Dissemination of Restricted Data.
 - h. (6) AR 381-3, Signals Intelligence (SIGINT) (U).
 - i. AR 381-11, Military Intelligence, Threat Analysis.
- j. AR 381-12, Subversion and Espionage Directed Against US Army and Deliberate Security Violations (Short Title: SAEDA).
 - k. (2) AR 381-12-1, Processing of SAEDA Incidents (U).
- 1. AR 381-14, Counterintelligence Technical Surveillance Countermeasures (U).
- m. AR 381-15, Military Intelligence, Domestic Exploitation Program (U)
- n. AR 381-20, Military Intelligence, US Army Counterintelligence (CI) Activities.
- o. AR 381-141, Military Intelligence, Provisions for Administration, Supervision, Control and use of Intelligence Contingency Funds (ICF): (U)

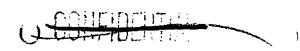
- AR 530-1, Operational Security (U).
- q. (U) AR 530-2, Communications Security (U).
- r. We AR 530-3, Electronics Security (U).
- s.(U) AR 530-4, Control of Compromising Emanations (U).
- t. AR 604-5, Clearance of Personnel for Access to Classified Defense Information and Material.
 - u. AR 604-10, Military Personnel Security Program.

DOD Publications:

- a. DOD 5200.1-R, Information Security Program Regulation.
- b. (SI) DOD 5200.1F (M-2) Special Security Manual
- c. DOD 5200.28-M, ADP Security Manual
- d. DOD 5220-22-M, Industrial Security Manual for Safeguarding Classified Information.
- e. DIAM 50-3, Physical Security Standards for Sensitive Compartmented Information Facilities.
- 3. Field Manuals:
 - a. FM 19-30, Physical Security.
 - b. FM 30-17, Counterintelligence Operations.
- 4. ACSI, DA Publications.
 - a. OACSI Sensitive Installation and Unit List (SIUL).
 - b. AARGRAMs (as applicable).
- 5. USAINTA Publications.
 - a. USAINTA Reg 10-2, Organization and Functions Manual.
 - b. V(g) USAINTA Reg 381-1, ICF (U)
 - c. USAINTA Reg 381-100, Counterintelligence Activities and Procedures.
 - d. Vs/ USAINTA Security Support Bulletins (U).



- e. (5) USAINTA Security Support Program Manual "THREAT" (U)
- f. 7(c) USAINTA Security Support Program Manual "Operations" (U)
- g. USAINTA Security Support Program Computer Security Manual.
- h. USAINTA Daily Operational Reports (as applicable).
- i. USAINTA Supplement to AR 380-5.
- 6. 902d MI Group Publications:
- a. 95) 902d MI Group Pamphlet 380-2, Security, SATRAN Reports (U).
 - b. 902d MI Group Daily Operational Reports (as applicable).



APPENDIX B TO 902D MI GROUP PAMPHLET 381-3

ESSENTIAL ELEMENTS OF INFORMATION (EEI)

GENERAL: In devising EEI applicable to the supported installation, each one of the multi-discipline threats must be examined in conjunction with the mission and situation of the particular target. The actual or potential vulnerabilities thereby conceived become REI affecting the supported installation. Since each installation has its own specific situation, it is imperative that the DSSA work very closely with a representative of the supported installation in order to arrive at an EEI listing tailored to the specific needs of the command. The references listed at APPENDIX A provide background information and guidance in devising EEI. Many of the areas covered by these references, which heretofore have been of little concern to the Special Agent, are now essential elements of knowledge to the DSSA if he is to successfully accomplish his mission under the DSCCP concept. This is particularly necessary in the areas of SIGINT, PHOTINT, OPSEC and Computer Security, Listed below are sample EEI for each category. These EEI are basic and are only a partial listing provided as an aid in developing a list peculiar to the supported command. Some of the items may not be germane to every DSSA but are included as nuclei for possible development of new or related ideas. The final EEI list prepared by the DSSA should include the source or sources that can provide the required information.

2. HUMINT: The following elements are those normally attributed to collection or exploitation by human intelligence sources. The information will usually be obtained by various HUMINT sources, personal observation by the DSSA and liaison contacts:

- a. HOIS subscriptions or regular acquisition of local and post newspapers and periodicals. Sources: LNO contacts and USAINTA.
- b. Deliberate compromise of classified information or unauthorized release of military information to representatives of foreign governments (ARs 380-5, 380-10, 381-12 and 381-12-1)
- c. Public information releases and local newspaper articles revealing unclassified but useful (to HOIS) information regarding the command.
- d. Theft, suspected theft, or unauthorized reproduction of classified documents and or material.
- e. Reported or suspected blackmail or coercion of individuals employed within the supported command.

REGRADED UNCLASSIFIED
ON SEP -5 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R



- f. Actual or attempted physical breaches of restricted area perimeter security, external or internal.
- g. Barly detection of persons whose activities and/or character weaknesses may render them vulnerable to hostile intelligence exploitation. Suitability factors may include:
 - (1) Breasive indebtedness or recurring financial difficulties.
 - (2) Unexplained affluence.
- (3) Conduct rendering the individual vulnerable to pressure, such as homosexual, criminal or immoral acts.
- (4) Excessive use of alcoholic beverages or improper use of drugs or marcotics.
 - (5) Mental or emotional instability or history thereof.
 - (6) Those who attempt to commit suicide.
- (7) Drastic changes in behavior to indicate possible unexplained pressures being brought to bear.
- h. Personnel who regularly and voluntarily work during non-duty hours when unobserved access to classified data is possible.
- i. Sudden unexplained or inadequately explained absences from work.
- j. Membership in, or association with members of organizations constituting a local threat against the US Army as defined in AR 380-13.
- k. Unsolicited correspondence from individuals, organizations or addressees known to be a threat to the US Army.
- 1. Allegations or denunciations of espionage or sabotage on the part of sensitive installation personnel.
- 3. PHOTINT: This pertains to intelligence obtained by means of photography, mainly through HOIS satellites or HOIS commercial aircraft. Also included must be threats posed by hand-held cameras operated from low-flying private aircraft and ground-level photography conducted from areas outside the perimeter of the installation. Photography from seaborne platforms should be considered at installations located near international waters. Sources of information for this type of data are documentary sources such as SATRAN messages, schedules of tests, operations and troop movements, as well as results of liaison contacts and personal observations. Some sample EEI are as follows:

F 52 H 1 L

REGRADED UNCLASSIFIED
ON SEP -15 1997
BY CDR USAINSCOM FOI/PO
AUTH PARA 1-603 DoD 5200.1-R



- a. Following activities during periods of scheduled overflights by HOIS satellites and commercial aircraft:
 - (1) Large and significant training exercises.
 - (2) Testing of equipment and/or techniques in the open.
 - (3) Uncamouflaged new or sensitive equipment.
 - (4) Other significant movements and activities.
- (5) Concentration of transportation equipment, i.e., transports, etc.
 - b. Build up of major item stockpiles in the open.
 - c. Gradual build up of facilities at a test site.
- d. Repeated violation of air restricted zones by commercial/private planes.
- e. Appearance of private aircraft during classified, or significant tests/demonstrations.
- f. Placing, operating or testing of new, significant or classified equipment in areas exposed to the public.
- g. Sudden appearance of camera-carrying "tourists" in the vicinity, coinciding with the scheduling of new, unusual and/or classified activity.
- h. Unobstructed windows and apertures in areas where classified matters are handled, permitting observation and photography from uncontrolled areas.
- i. Foreign Vessels, particularly from East Bloc Countries, appearing off-coast of installations near international waters.
- 4. SIGINT: Signal intelligence is derived from the intercept and analysis of communications, COMINT, and from communications electromagnetic radiations, ELINT. HOIS SIGINT collection against US facilities is accomplished from air-borne, sea-borne, and land-based platforms. HOIS capabilities in this field are described in the USAINTA Threat Manual and additional information as to specific threat to the supported installation may be found in reports of SVAs and SAVEs and/or requested from USAINTA. The field of SIGINT is a very complex and specialized one. Adequate protection of a command/installation from HOIS SIGINT collection requires.

REGRADED UNCLASSIFIED
ON SER USAINSCOM FOLIPO
BY COR USAINSCOM FOLIPO
AUTH PARA 1-603 DOD 5200.1-R

COMPISENT

the application of Signal Security (SIGSEC) which includes Communications Security (COMSEC), and Electronic Security (ELSEC). COMSEC measures are applied to telecommunications systems and has four components; crypto security, physical security, transmission security and emmission security. ELSEC pertains to protective measures applied to electromagnetic radiation of non-communications equipment and systems to prevent the interception, analysis or exploitation of those radiations by foreign intelligence. The DSSA must become sufficiently familiar with the above subjects in order to recognize vulnerabilities, and know when to recommend a request for technical assistance. References lh, l, p, q, r, s, and 5d and e in APPENDIX'A will provide additional information. Purthermore, the DSSA must work closely with the staff element having responsibility for SIGSEC of the supported installation. The EEI selected will be the type that can be fulfilled by human sources, preferably located in communication/electronics work areas. Some EEI common to SIGINT are located in para lc, Appendix to AR 530-1. Other sample EEI follow:

- a. Conducting tests on new or sensitive radars and other non-communication emmitters within range of land based, air-borne or sea-borne HOIS ELINT platforms.
- b. Installing and operating electrically operated, informationprocessing equipment which handles classified information without the application of compromising emanations control measures.
 - c. Poor telephone security to include:
- · (1) Discussion of classified matters over Autovon and commercial telephone systems.
- (2) Discussions of upcoming events which can provide tipoffs to classified activities.
 - (3) Use of double talk in reference to classified messages.

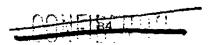
(4) Reading/quoting verbatim portions of classified matters.

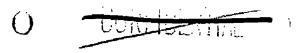
5. OTHER EEI: The following items are of interest to the US Army intelligence community and will be forwarded to this headquarters by

Agent Report format for appropriate action. A statement in Agents Notes will indicate if and how the information has been reported through other appropriate channels. As the information will be passed to USAINTA for possible exploitation bt the Special Operations Detachment or the Director of Operations as appropriate, the Agent Reports will be classified CONFIDENTIAL-NO FOREIGN DISSEM. Normally this information is not passed to the local commander other than to insure that other proper reporting

REGRADED UNCLASSIFIED

ON SEP -5 1980M FOI/PO BY CDR USAINSCOM FOI/PO AUTH PARA 1-603 DOD \$200.1-R





procedures are being followed by the command.

- a. Identification and extent of foreign contacts of military and DOD civilian personnel, with emphasis on Soviet bloc countries.
- b. Intended foreign travel of military or DOD civilian personnel to Soviet bloc countries or attendance at social or official functions at which Soviet bloc countries are present.
- c. Foreign business or professional connections and the extent thereof of military and DOD civilian personnel and their families, with emphasis on Soviet bloc countries.
- d. Solicitation by foreign national or organizations of personal or official information through official or unofficial channels.
- e. Invitations by non-US Government organizations or individuals to members of the supported command to Participate in conferences or symposia or to submit papers for publications in professional journals on activities related to their government employment.

REGRADED UNCLASSIFIED

ON SER 15 1985M FONPO
BY COR USAINS DOD 5200.1-R

AUTH PARA 1-603 DOD 5200.1-R



APPENDIX C TO 902D MI GROUP PAMPHLET 381-3

DSCCP QUARTERLY PROGRESS REPORT

- 1. (U) IDENTIFY: (Name of 902d MI Group Field Element providing support).
- 2. (U) SUPPORTED COMMAND: (The activity(ies) receiving the support and the major command(s) involved.)
- 3. () TARGET ANALYSIS: (In the initial report summarize the results of target analyses conducted for all activities, installations, or separate elements designated and included in the program, by order of priority of support. Subordinate elements large enough to be designated sub-targets will be listed in subparagraphs. In subsequent reports, indicate only changes as they occur.)

4. () QUARTERLY BRIEFING OF SUPPORTED COMMAND

- a. Circumstances: In brief narrative form, cite date(s), identities of all persons present, and subjects discussed and results of the briefing(s).
- b. Recapitulation of Operational Progress During the Period: In as many subparagraphs as may be required, cite significant developments as pertain to development of the program, improvements in target coverage, and any operational readjustments made during the period. In citing specific items of interest, identify each by making reference to the appropriate reports made during the reporting period which contained details of the topic discussed with the commanders, if applicable.
- c. Significant Counterintelligence Information Developed: In as many subparagraphs as may be required, cite identities of personalities, incidents, or groups discussed with reference to the report previously submitted.

5. () INFORMATION SUBMITTED:

a. To the local commander and actions implemented or taken as a result:

Subject Type Information Developed Action Taken Date of Action

b. To the intelligence community;

Subject Type Information Developed To whom reported

6. () COMMENTS, REMARKS AND RECOMMENDATIONS:

In this paragraph, indicate any general remarks or indications of special

interest shown by the supported command that are not covered in above paragraphs. These remarks should reflect the commander's assessment of the viability of the program, whether it is meeting the objectives and achievements as he sees them, and any problems and/or recommendations. Also indicated the extent with which the commander or his representative has cooperated with the FO/RO and/or this group and any pertinent remarks which could serve to improve the DSCCP support to the command. Where problem areas have been encountered, findings and recommended solutions will be provided. Lessons learned should be included to assist in the planning and implementation of other operations. A statement will be entered as to whether any information concerning non-affiliated DOD civilians or organizations was reported (AR 380-13). If affirmative, reference specific report or attach copy. Utilize subparagraphs to explain or amplify information or data reported.

NOTE: Classify each paragraph according to its content. Because of the distribution of this report, care must be taken to insure that the contents of the report do not reveal SI/SAO access material. An example of this would be to include the Statement "three items of PHOTINT information, reference messages _____, and _____, were received and passed to the supported command. Appropriate actions were taken", without revealing the SI/SAO information contained within the reference messages.