~~CONFIDENTIAL~~

DEPARTMENT OF THE ARMY
US ARMY INTELLIGENCE AND SECURITY COMMAND
FORT GEORGE G. MEADE, MARYLAND 20755

FEB 9 1979

IASO-SA

SUBJECT: Report of Internal Counterintelligence Program (ICIP) Operation (U)

HQDA (DAMI-CIC/Ms Brannan)
WASH DC 20310

1. ~~(C)~~ (U) Submitted herewith is the status report, 1st Quarter, FY 79, for ICIP Operation LENTIL MONKEY (U). During the reporting period the operation produced two Summaries of Information, one Source Lead Development Report, 35 Contact Reports and 40 Agent Reports.

2. ~~(C)~~ (U) LENTIL MONKEY (U), supporting the Defense Language Institute, Foreign Language Center (DLIFLC), Presidio of Monterey, CA, is the only CONUS ICIP being conducted. However, the type information generally developed from the project, and this Command's current investigative and reporting authority, suggest that a different type program would be better suited to provide the required security assistance for DLIFLC. A Dedicated Operations Security Support Program (DOSSP) could effectively replace the ICIP without employing confidential sources and be readily implemented by the 902d Military Intelligence Group with existing personnel assets. At inclosure two is an extract from the USAINSCOM OPSEC Support Procedures Manual which describes the DOSSP.

3. ~~(C)~~ (U) The general concept and recommendations to replace ICIP LENTIL MONKEY (U) with a DOSSP have been discussed and concurred in by the Commandant and Security Officer at DLIFLC. The operational concept would be tailored to satisfy local security requirements unique to DLIFLC.

4. ~~(C)~~ (U) In view of the above, request authority to terminate ICIP LENTIL MONKEY (U). Concurrent with termination of the ICIP, a DOSSP for DLIFLC will be implemented.

William I. Jennings

2 Incl
as

WILLIAM I. JENNINGS
Special Assistant (OPS)

CLASSIFIED BY CDR INSCOM
REVIEW 8 FEB 99
EXTENDED BY CDR INSCOM
REASON Para 2-301.3.c.

858
858

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

~~CONFIDENTIAL~~

III. TYPES OF SUPPORT

1. GENERAL: This section discusses the various types of OPSEC support that are available within USAINSCOM. It should be noted that operations security is a command responsibility. Therefore, any improvements in the supported commands' OPSEC posture must be accomplished by the supported commander. USAINSCOM is unique in that the present organization integrates many of the counterintelligence/security skills that formerly were assigned to separate Army commands. As such, the Commander, USAINSCOM, has the capability to conduct a multidisciplined security evaluation of a project, activity or facility. With the divergence of skills integral to the USAINSCOM organization, the majority of problem areas that have been historically associated with OPSEC can be addressed, and with the multidisciplined approach, USAINSCOM units are able to assist supported commanders by evaluating their OPSEC posture and recommending means of improvement. This should enable the achievement of a much better security posture. The following paragraphs describe the types of support which USAINSCOM units provide.

2. [redacted] PROGRAM (DOSSP):

2-1. The DOSSP Concept: The DOSSP is a systematic, ongoing, dynamic approach to providing the local commander, operations security officials, project managers and security managers of US Army installations/units/activities/projects with meaningful operations security support in the form of timely, accurate, all source intelligence information pertaining to the real-time, multidisciplined threat posed by hostile intelligence; observed vulnerabilities of the supported element to that threat; and recommendations for appropriate corrective action to enhance operations security. This program is based on a Covering Agent (CA) in an overt continuous role of acquiring information about the supported activity and the threat thereto and providing it to the supported activity in a timely manner, while concurrently recommending practical "fixes" to reduce observed vulnerabilities.

2-2. Responsibilities: Implementation of the Dedicated Operations Security Support Program is the responsibility of each individual field element (RO/FO/Detachment) within the policies provided by the HQ, USAINSCOM. Responsibility for supervision, guidance, and comprehensiveness, rests with the Field Offices, Detachments, and Battalions within their respective areas of responsibility. Group Headquarters will provide guidance, as appropriate, monitor the overall program, acquire and disseminate threat data, and, in the case of certain key projects/activities which stretch beyond local boundaries, will provide centralized management of the overall DOSSP effort.

2-3. Target/Project Selection: Determination of who should be a recipient of DOSSP support is a continuous process of initiative, investigation, and evaluation. Such documents as the ACSI Sensitive Installation and

859

Unit List and other sensitive activities listings are helpful, but not comprehensive. Each field element must do all within its capabilities to insure they are aware of all significant Army activities in their AOR. Once this grasp of the local environment is obtained, prioritization based on available manpower, desires of supported activities, information from intelligence channels, and perceived security sensitivity of the supported activity is made to determine if DOSSP support is appropriate. Security sensitivity is the most important aspect in determining if an activity requires support. Determination of security sensitivity must be based on the importance of the activity to US national security as well as the potential benefit to be derived by a hostile element if they were to obtain details about the activity.

2-4. Covering Agent Functions:

a. Threat: The Covering Agent must be an expert in the threat to the activity he has been detailed to support. This can be accomplished only by thorough study of national threat data, review of periodic intelligence updates, and liaison with local, state, and federal agencies, as well as their foreign equivalents, where appropriate, in order to develop local threat. Refinement of this threat to manageable size is based on a thorough knowledge of the supported command.

b. Knowledge: OPSEC support to an activity is predicated upon a thorough knowledge of that activity. There is no easy way to obtain this knowledge other than extensive research into the organization's mission, functions, and organization. An initial step in this direction is the reading of Army Regulations and Field Manuals pertaining to the activity. Briefings from activity personnel, study of organization and functions manuals, test plans, contingency and operations plans, and related documents are the means for building a comprehensive data base. Even after building this initial base, a systematic plan for obtaining data on an on going basis should be instituted, i.e., daily bulletins, test schedules, briefings, and test plan changes. While expertise in SIGSEC and IMAGERY Security by CI Agents is not required, familiarity with basic concepts is. A primary goal of the USAINSCOM OPSEC Support Program is to provide Army elements a single point of contact for obtaining MI support, be it SIGSEC, IMAGERY Security, or Counterintelligence.

c. Execution: Success in the OPSEC support area is based on the willingness of the covering agent to cast himself in the role of an all source agent and his innovative application of investigative skills in developing threat and vulnerability data, use of deductive reasoning, common sense, and gaining the confidence and respect of the personnel of the supported command. If the confidence of workers at all echelons of the supported command can be gained, their willingness to provide candid assessments of vulnerabilities within the activity will become the Covering Agent's best asset. The CA may know a lot about an activity, but the actual workers know a great deal more. Their experience makes them much more able to relate security weaknesses if they appreciate the threat.

d. Recording: Methodical recording of threat, vulnerabilities, unusual incidents, ideas, and recommendations is essential in building a successful DOSSP. This allows the CA to evaluate comprehensiveness of local hostile intelligence targeting, determine patterns, and fit together isolated incidents, and provides continuity of support as personnel are transferred. ~~A sample workbook is included as figure 1.~~

e. Reporting: Other than the maintenance of workbooks, no formal reporting requirements are imposed on covering agents except in extenuating circumstance of intense, critical stages of support. CA's will keep the chain of command informed of significant activities.