28 February 1973

MEMORANDUM FOR: Chairman, Computer Security Subcommittee

SUBJECT : Security Policy Guidance Required by CIA for ADP Operations

I. General:

The policy paper should stress the systems approach toward security of ADP systems. This means that the various facets of consideration; personnel, physical, procedural, software and hardware, should be interdependent to the point where a breakdown in one aspect would be covered by another, i.e., a breakdown in physical security would be immediately correctable prior to any compromise by personnel or procedural measures.

There is a feeling in some parts of CIA that the "dreamed of" goal of someday attaining security in multi-level operations ~~is~~ may be impossible. Thus, it is felt that all of the above categories of ADP security should be given equal attention. It should be stressed that security features of the total system should be practical and should be repeatedly tested. There should also be a program of

thorough indoctrination of ADP personnel with a follow-up reindoctrination program on a timely basis.

A. Sanitization - guidance on sanitization of storage media should be issued as soon as possible. This guidance should include some degaussing procedures which can be followed in the event an ADP systems manager is confronted with defective core, plated wire, etc.

B. Security Labels - guidance is needed on methods of including internal security labels which will be printed out at the terminal and/or displayed on the scope with the data as it is accessed. Further, policy guidance is needed on how this should be accomplished to be in accordance with the new Executive Order 11652. This policy should also cover the necessity of assuring that portable storage media such as tapes and disks are properly labeled prior to removal from computer center control. These labels should, of course, agree with the internal labels recorded on the media.

C. Fetch Protection - policy guidance is needed to protect storage areas after one user has signed-off and the next user

logs-on. In other words, the next user using that storage area should not be able to access any residue data left by a previous user. Where fetch protection is not technically feasible, some other method should be devised.

D. Audit Trails - guidance is needed in the development of audit trails and the use of these audits. Should the security officer be the reviewing official of these audit trails? Should the audit trail be reviewed daily, weekly, etc.? Should there be a method by which the audit trail or some companion software package immediately alerts the operator? the security officer? or some other official immediately at the time of a possible security violation? How much data should the audit trail gather?

E. Other -

1. Policy guidance is also needed in the purchase of new systems. Which systems are likely to be able to meet the minimum security requirements necessary to operate in a compartmented mode?
2. What methods of remote terminal identification would be acceptable? Must terminals be hard wired and

identified by terminal number; could they be identified by line or would software measures be acceptable? Should features be incorporated in the system which will automatically cut off the terminal after a certain number of false attempts to access the system have occurred? Or should these instances be recorded in an audit trail and investigated at a later date; within 24 hours; within a week, etc.?

3. Should critical personnel associated with the ADP processing components be singled out for more in depth investigations prior to employment? Should these personnel be reviewed more often than other employees? Who are these personnel? How much physical security protection for each computer area is necessary in an environment such as the CIA building which has 24-hour guard protection both inside the building and on the building's perimeters? Is there a less expensive answer to this question than the construction of vaulted areas?

4. There is a very serious need for more specific guidelines in the area of EMSEC. It is suggested that this Committee attempt to work in close coordination with COMSEC elements of the Intelligence Community to develop these guidelines as soon as possible.

STAT

CIA Member
Computer Security Subcommittee