28 February 1973

MEMORANDUM FOR: Chairman, Computer Security Subcommittee (USIB)

SUBJECT: USIB Computer Security Policy Paper

1. Reference: Proposed Outline, IC Computer Security Policy, submitted to the CSS by the Army member in December 1972.

2. Reference outline contains the types of information and guidance we believe should be included in subject policy paper. The following comments clarify and amplify the items listed in the outline:

a. The computer systems to which the policy paper applies should be clearly identified (e.g. only intelligence systems which process compartmented intelligence, only those systems which operate in a compartmented mode, etc.).

b. In addition to the definitions in DCID 1/16, recommend inclusion of: facilities accreditation (as distinguished from system accreditation), ADP system security, dedicated mode, multilevel security mode (as distinguished from compartmented mode), central computer facility, remote terminal facilities, compartmented intelligence, and collateral intelligence.

c. The policy portion of the paper should address the following areas:

(1) The options for processing compartmented intelligence:

(a) System dedication. (Permanent and temporary)

(b) System splitting.(multi-processer systems)

(c) Compartmented mode.

(2) Assumptions to be made when designing and installing ADP security systems. (Not to include the assumption that your system has been penetrated by a hostile intelligence organization)

(3) Responsibilities of USIB members in the areas of ADP system testing, evaluation, accreditation, and delegation of authority.

(4) Responsibility for accrediting networks.

(5) Minimum requirements for all ADP systems which process compartmented intelligence, regardless of processing mode:

(a) All computer center personnel cleared for TOP SECRET information and with access authorizations for all compartments of information stored and/or processed in the system.

(b) The computer center facility accredited for processing the most sensitive compartmented information in the system.

(c) All personnel accessing the system from outside the computer center cleared for TOP SECRET information, but not necessarily for all compartments of information in the system.

(d) All remote terminal facilities of the system maintained, at a minimum, as controlled TOP SECRET environments.

d. Security Requirements.

(1) Recommend a comprehensive list of duties and functions be included for ADP security officials: ADP System Security Officer, Computer Center Security Officer, Terminal Area Security Officer.

(2) Emphasize systems approach to security. In view of current security shortcomings of computer hardware and software, other conventional areas of security must be stressed (physical, personnel, procedural, communications, and emanations security). Hardware/software security features can be relied upon principally to protect NEED-TO-KNOW.

(3) Examples of useful security measures/constraints to reduce the security hazards in ADP systems should be provided, such as:

(a) Elimination of programming and data base update capabilities from remote terminals which are not cleared for access to all compartments of information stored and/or processed in the ADP system. Such terminals might be restricted to query and retreival languages only.

(b) Automatic terminal lockout after a limited number of attempts to log on the system or to provide a proper password when interrogated by the system.

(c) Automatic terminal lockout when an on-line terminal is inactive for a specified period of time and the last user has not logged-off.

(d) Possible use of "front end" computers to service user requests and verify user authority to access programs, files, etc.

(e) Use of testing teams and spy programs.to evaluate system security.

e. Accreditation Procedures.

(1) Facilities accreditation, and the procedures to acquire it, should be clearly distinguished from system accreditation (mode of operation).

(2) This section of the policy paper should incorporate an updated version of USIB-D-71.9/2, 7 April 1971, " Guidlines for the Security Analysis, Testing, and Evaluation of Resource-Sharing Computer Systems."

John C. Karp Jr.

JOHN C. KARP, JR
Major, US Army
Army Member