



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, D.C. 20350

~~CONFIDENTIAL~~

IN REPLY REFER TO
Op-092D222/joy
Ser 03170P092
24 SEP 1970

~~CONFIDENTIAL~~

MEMORANDUM FOR THE CHAIRMAN, COMPUTER SECURITY SUBCOMMITTEE
OF THE UNITED STATES INTELLIGENCE BOARD

Subj: Minimum Security Requirements for Compartmented
Operations of Remotely Accessed Resource-Sharing
Computer Systems in a Controlled Top Secret
Environment (C)

1. (C) The proposed directive which would establish security requirements relative to the processing of sensitive compartmented information in computer systems has been reviewed. This office concurs in the concept of the basic proposal but nonconcur and submits a recommended change relative to the physical security and personnel clearance requirements for remote terminals.

2. (C) In regard to remote terminals, it is recommended that the security requirement be changed to only require that remote terminals be afforded physical security and cleared operating personnel appropriate to the classification level of input/output designed for the respective terminal, which could be less than Top Secret. To emphasize the need for this recommended change, as the Navy adds to and modernizes its current 1,001 computer installations, planning is to procure new systems that will service the computer needs of an entire ship or naval base. Such centralization of computer usage is considered necessary in the interest of efficiency and today's austere operating budget and besides it will allow more extensive use of computers with the available multi-purpose computer justifying the computerization of many smaller ship or base functions. Since such a shipboard or base computer will be handling operational, supply, intelligence and personnel functions, the classification of input/output for the system could range from unclassified to sensitive compartmented information with the majority of the users operating at the Secret or lower level. Thus the question of security clearance and access control requirements for remote terminals becomes critical and it is impossible, in view of the additional personnel security investigations and

GROUP 1
Excluded from automatic
downgrading and
declassification

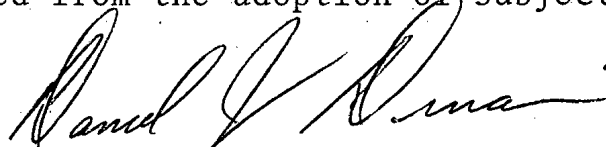
*REC'D: IPB
1 OCT 1970
RB*

~~CONFIDENTIAL~~
~~CONFIDENTIAL~~

CONFIDENTIAL* **CONFIDENTIAL**Op-092D222/joy
Ser 03170P092

physical security costs, to concur in a policy that would arbitrarily require the protection of a remote terminal at the Top Secret level instead of according to its input/output, especially when it is considered that other requirements in the proposed directive would limit the possibility of unauthorized disclosures to terminals.

3. (C) Additionally, it is strongly recommended that the Computer Security Subcommittee take advantage of the momentum this task has generated to now develop a flexible and realistic computer security policy that encompasses all classified intelligence information. In view of the greater number of computer systems to which such a policy would apply and the potential for improved security, compatibility between agency data banks and monetary savings could be significantly more important than the results to be expected from the adoption of subject draft.



DANIEL J. DINAN
Head, Security Policy Branch
ACNO (Intelligence)

CONFIDENTIAL**CONFIDENTIAL**