DDS&T #2378-70
1 July 1970

MEMORANDUM FOR: Director of Security

SUBJECT : Comments on Proposed DCID entitled "Minimum Security Requirements for Multi-Level Operation of Resource Sharing Computer Systems in a Benign Environment"

1. I agree with the intent, the security concepts, and with most of the proposed requirements of the proposed DCID, but I do not concur in the draft in its present form. My main criticism is in the wording of several sections--more specifically with three areas of definition which need more careful and precise language before a policy of such far-reaching consequences is promulgated:

--The computer environment for which the policy is to apply is not described consistently throughout the paper.

--The term "multi-level" is not used consistently. Indeed the concept of security "levels" is not clear.

--The words used in the draft to describe requirements relating to authorization to use these computer systems are not applied with sufficient care.

2. The specific comments below deal mostly with such questions of wording. The draft is a good start; particularly noteworthy is the absence of technical jargon. I believe the necessary time should be taken to do a good editing job, regardless of deadlines previously established.

a. The paper fails to distinguish clearly between the use of a computing system in which the user has remote

access and the operation of a closed-shop computing center in which the normal operating system being used allows for the running of more than one program concurrently. This problem is illustrated in the first definition on page 7: The terms "multiprogrammed" and "multiprocessing" are used; these terms do not necessarily imply "remotely accessed". Again on page 14 the term "remote batch mode" is used and specific requirements are stated for this method of operation, as distinguished from the interactive terminal mode. The reasons for this distinction are not given; indeed the definition of remote batch mode is not given anywhere in the paper. It is imperative that the environment for which the policy is to apply be more precisely defined before OCS attempts to judge the practicality of some of the requirements. For example, our ability to meet the user identification/authentication requirements (para. 6 (b), page 14) depends on whether the environment is defined to include multi-programming.

b. At some points in the paper there is an attempt to distinguish between "multi-level" and "compartmented" information. At other points the distinction between these two terms is not made. The wording used at the beginning of paragraph 6 (page 13) is an illustration of the confusion which results from an attempt to distinguish between "levels" and "compartmentation". If interpreted literally, the requirements of this paragraph would not apply to compartmented data at the same security level. Another example of the confusion is in paragraph 3 (Physical Security Protection) on page 12. It is stated that "the computer center area requirements shall be based on the highest level of the total system; remote terminal area requirements depend on the highest level of information designated for input/output at each terminal." But paragraph 3, page 7, says a benign environment is one with protection and control at the top secret level. If the "highest level" of data is below top secret, which of the two statements applies? The same

question could be asked concerning the requirement for protection of communication links at the top secret level (page 12) if the data to be transmitted is below that level. The use of the term "multi-security level" on page 2 confuses the matter further. The need for two different terms--"multi-level" and "compartmented"--is questionable. The important point is to provide for adequate separation of information within a system when creators or users of such information feel that such separation is necessary. Perhaps the term "compartmentation" or "compartmented information" is adequate in all the appropriate places in the paper in lieu of "multi-level".

c. The following terms are used in the paper to denote the concept of authorization to access the computer system: access authorization (page 11), authentication (page 11), access control passwords (page 11), access approvals (page 11), designated personnel (page 12), user identification/authentication (page 14), authorization codes (page 14), authorized requestor (page 14), access control (page 15), passwords (page 15), user access list (page 15), access limitations (page 16), user authorization (page 16). In some cases these words are used as synonyms, in other cases one can infer that there is a distinction between these words.

d. The paper is addressed to the "benign environment", but in some places the paper implies the need for protection against "deliberate unauthorized intrusion" (page 6) and "unauthorized probes" (page 14). The connotation of "benign" can be misleading; perhaps a better choice is "non-hostile".

3. The most crucial part of the proposed DCID is paragraph 6, beginning on page 13. Specific comments are made below on each of required features (as identified by sub-paragraph):

a. Although detail is given on the requirement to include security indicators, there is no purpose given for this requirement.

b. The wording used in the initial sentence of this paragraph is much too confusing; it needs to be simplified. The special requirements noted for "remote batch mode" should be stated differently so they will apply for all remote users. That is, if there are procedures which permit the user to leave the area while the computer is still working on his task (regardless of the kind of terminal involved), there also should be a procedure to insure that the computer output is delivered only to him when he returns. Finally, the requirement to identify a specific user with a specific terminal will be unwieldy in CIA Headquarters since it is intended that terminal "service centers" be established for general use of anyone in the area. Also the practice of going to the nearest available terminal has already been well accepted and the security procedures now in force seem to provide adequate control.

c. This requirement assumes that core is shared among several user programs. Under some operating systems this may not be the case. More importantly, OCS cannot meet this requirement for most of its equipment without special changes made by the manufacturers

d. The wording of this requirement, as well as others to be met by hardware functions, tacitly assumes that verification of correct operation of these functions is not only possible but also practical. To the contrary, this is a substantial effort in its own right. This is true both of the initial verification that the features do in fact operate as they are designed to operate and also for the continuing inspection of these features to determine that they have not been subverted or circumvented. Rather than use the strict language proposed, it might be better to state these as explicit design goals and add a general statement elsewhere on the hardware/software reliability problem.

SUBJECT: Comments on Proposed DCID

e. The wording used here needs to be drastically revised: what does the term "independent hardware" mean? How is "disposable residue" distinguished from "undisposable residue"? What is meant by the term "auxiliary memory?"

f. The word "software" on the second line should be deleted. The use of the term "selected" implies that some files can be used without any "access control". Is this correct? OCS cannot adequately meet the requirement for controlling read/write authority with its present software nor with any other known software suitable for its environment.

g. To obtain a "complete listing of personnel attempting to gain access" would require the cooperation of hostiles. The last sentence of this sub-paragraph might better be included under the security officer duties on page 11.

h. The "direct control" to be exercised by the system security officer in modifying software security features is impossible to guarantee; no one can make the claim that an operating system can be rendered completely invulnerable to attempts to modify it by user programs. The intent of this paragraph should be retained, but it should be reworded to take into account the current state-of-the-art in operating systems.

4. The proposed maximum delay in effecting this policy (1 January 1971) is impractical for OCS and perhaps other centers in CIA as well. While most of the requirements of this proposed directive have been or can be met, there needs to be sufficient time for training security personnel, computer users, and system designers, and to insure that all provisions of this directive are being applied in fact as well as in spirit.

/s/

CARL E. DUCKETT
Deputy Director
for
Science and Technology

cc: C/IP Board

9 July 1970

TRAINING

Because the numbers of ADEPT students destined to become full-time computer programmers had been lessening with each running of the course, it was decided to review the goals and selection criteria for enrolling students in the 15-week OCS course in basic programming (ADEPT).

It was decided to initiate a more modest 5-week course "Introduction to Computer Programming" beginning 9 Nov 1970 to be slanted toward those who needed in depth knowledge in programming but were not being groomed for full-time programmer jobs. The IPC's of all directorates were advised to screen applicants for both courses by administering the Brandon-Wolfe Test (Aptitude Assessment Battery: Programming) and the IBM Programmer's Aptitude Test (PAT) to help determine the individual's potential and performance and use results of these tests in making selections for the two courses; and also that attendance at the 15-week ADEPT course be limited to those expected to fill positions as full-time computer programmers.

PLANNING QUESTIONNAIRE

10 July 1970

Response to a customer questionnaire relating to their usage of remote terminals in the interactive computer system brought out the following information:

Uses being made of the system:

Programming tasks	47	customers
Information retrieval	38	"
Calculations	30	"
	115	

Customers were asked, in view of the cost of the 360/67 of [redacted] whether their experience so far had been satisfactory or not. Replies were as follows:

7		Has not paid off and intend to stop terminal use
10		Has not paid off but have no alternative but to continue using it
22		Has not paid off yet but expect it will
48		Has paid off but needs improvement
24	(11)	Has paid off and basically satisfied with system

Note, 75% indicated the system was paying off for them.

One of the principal complaints was need for better, or more consistent, response time, in order to increase the payoff of the interactive services.

A good deal of information was received from the customer replies which was helpful in planning for the future.

COINS 5 August 1970

Current participation in COINS limited to 3 hrs a day on the IBM 360/67. This costs about [redacted] STAT besides which the system is lost to those Agency components which had begun to depend on it for on-line program development, file handling and computational support.

STAT [redacted] recommended the Agency acquire a separate computer to be devoted to COINS and other external access applications full time. He assumed the Director of Security would continue to ~~desire~~ advise against storing Agency-sensitive data in a computer which has a possible data path to an uncontrolled terminal. It appeared that two distinct physical systems would be necessary, principally to avoid the risk of sensitive Agency data accidentally being disclosed outside the Agency.

STAT [redacted] felt the CRS should operate the COINS computer, and should have the choice of selecting the type of computer and developing the software.

STAT 10 Aug 1970, [redacted] recommended placing the burden of security on the individual agency through procedures which would